Простое руководство по установке и использованию Windows Server 2003

Windows® Server 2003 для "ЧАЙНИКОВ"™

Для сомневающихся

Освойте методы управления учетными записями пользователей, проектирования и обеспечения безопасности сетей

Эд Титтел
Джеймс Майкл Стьюарт

WILEY

ДИАЛЕКТИКА

Windows® Server 2003 FOR DUMMIES®

by Ed Tittel with James Michael Stewart

WILEY

Wiley Publishing, Inc.

Windows® Server 2003 для "ЧАЙНИКОВ"™

Эд Титтел,
а также Джеймс Майкл Стьюарт

ДИАЛЕКТИКА
Москва • Санкт-Петербург • Киев
2004

ББК 32.973.26-018.2.75
Т45
УДК 681.3.07

Компьютерное издательство "Диалектика"

Зав. редакцией *С.Н. Тригуб*
Руководитель проекта *В.В. Александров*
Перевод с английского и редакция канд. техн. наук *В.М. Неумоина*

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

Титтел, Эд, Стьюарт, Джеймс, Майкл.

Т45 Windows Server 2003 для "чайников". : Пер. с англ. — М. : Издательский дом "Вильяме", 2004. — 368 с. : ил. — Парал. тит. англ.

ISBN 5-8459-0559-1 (рус.)

Эта книга посвящена Windows Server 2003 — одной из наиболее перспективных операционных систем и созданию сетей в этой среде. Она охватывает все вопросы управления компьютерными сетями, дает базовые знания сетевой терминологии, включая аппаратное и программное обеспечение. Вы познакомитесь с подробным описанием процесса установки и настройки сетевой среды Windows Server 2003. Книга представляет собой на редкость удачное сочетание учебного пособия и справочника, ее можно читать от начала до конца или открыть в любом месте и получить нужную информацию. Для чтения книги не требуется специальной подготовки, она написана простым языком, понятным непосвященным. Книга станет незаменимым пособием для тех, кто стремится самостоятельно освоить сложный мир сетевых технологий на примере самой современной сетевой операционной системы — Windows Server 2003.

ББК 32.973.26-018.2.75

ISBN 5-8459-0559-1 (рус.)
ISBN 0-7645- E633-7 (англ.)

Оглавление

Содержание

Об авторах

Эд **Титтел** (Ed **Tittel**) — ветеран издательского дела, в активе которого несколько сотен журнальных статей и больше 100 книг. Эд работал над несколькими книгами из серии ..."для чайников", включая *HTML 4 для "чайников"*, 3-е издание, *XML For Dummies* (совместно с Франком Бомфри (Frank Boumphrey), а также над книгами на другие темы. Эд председательствует в небольшой компании LANWrights (Остин, штат Техас), которая специализируется на обучении, консультациях и публикациях в области компьютерных сетей. В свободное время Эд любит расписать пульку, готовить и охотиться со своим Лабрадором Блэки. Адрес электронной почты Эда — etittel@lanw.com., а адрес его Web-страницы — www.anw.com/staff/etbio.htm.

Джеймс Майкл **Стьюарт** (James Michael Stewart) работает в сфере компьютерных технологий больше восемнадцати лет. Майкл — независимый консультант и инструктор, а также автор многих публикаций. Его работа в основном посвящена проблемам безопасности, Windows NT/2000/XP и Windows 2003, интрасетям и Internet. Майкл принимал участие в написании многочисленных книг, посвященных программам сертификации и администрирования компании Microsoft; его статьи опубликованы в обычных и электронных изданиях. Он является автором обучающей системы и преподавателем учебного курса по программе сертификации компании Microsoft. Кроме того, он регулярно выступает с докладами на форуме Networld+Intertop. Он дипломированный инженер по системам корпорации Microsoft (Microsoft Certified Systems Engineer — MCSE) и обладает следующими сертификатами: CISSP, TICSA, CIW Security Analyst, CTT+, CCNA, MCSE NT & W2K и iNet+. Майкл закончил Техасский университет в Остине в 1992 году со степенью бакалавра философии. В области компьютеров он самоучка, его знания основаны на более чем 18-летнем опыте. Свое свободное время он посвящает чтению, пешим путешествиям по Техасу, катанию на велосипеде и столярным работам. Адрес электронной почты Майкла — michael@impactonline.com.

Благодарности авторов

Как всегда, хотим поблагодарить сотрудников LANWrights, которые работали над этой книгой: Мери Бурмайстер (Mery Burmeister) и Кима Линдроса (Kim Lindros). Со стороны издательства Wiley Publishing особая благодарность Сьюзан Пинк (Susan Pink), Бобу Уорнеру (Bob Woerner) и Аманде Фоксворт (Amanda Foxworth). Я также хотел бы поблагодарить Джесона Зандри (Jason Zandry) за его крайне ценную и желанную помощь в окончательном рецензировании книги, а Майкла Стьюарта (Michael Stewart) — за его не менее желанную помощь в рецензировании более ранней редакции. Я хотел бы поблагодарить моих родителей за то, что они сделали мою карьеру возможной и достижимой. Наконец, я хочу поблагодарить мою невесту Дину Кутуеву (Dina Kutueva), которая вошла в мою жизнь, к сожалению, очень поздно. Добро пожаловать в Америку! Также спасибо Блэки, моему верному другу-лабрадору, который постоянно вынуждал меня оторваться от клавиатуры, чтобы взглянуть на мир.

— Э.Т.

Спасибо моему соавтору, Эду Титтелу, за то, что предложил мне работать над этой книгой, а также моему редактору Мери Бурмайстер за то, что заставила меня написать еще одну книгу. Хочу поблагодарить своих родителей, Дейв (Dave) и Сью (Sue), — спасибо за вашу любовь и постоянную поддержку. Спасибо Марку за то, что всегда был рядом. ХЕРберту (HERbert) и Куин (Quin) — за то, что перестали выслеживать котят по всему дому! И наконец, как всегда, спасибо Элвису (Elvis): если у меня портилось настроение, я вспоминал твой блестяший кожаный комбинезон с большим воротом — и катался по полу от смеха.

— Д.М.С

Введение

Книга *Windows Server 2003* для *"чайников"* поможет всем, кто не знаком с Windows Server 2003 (или компьютерными сетями вообще) и желает найти свой путь к освоению сетей на основе Windows Server 2003. В мире, опутанном миллионами километров проводов, сети обеспечивают связь, которая объединяет всех пользователей вместе. Если вы еще не используете сеть, вполне возможно, что в один прекрасный день вам придется начать делать это! Хотя некоторые счастливчики, может быть, уже познакомились с Windows Server 2003 и сетями, большинство из вас не только ничего не знают о компьютерных сетях, но и откровенно напуганы ими. Тем, кто обеспокоен возможностью встречи с новыми и трудными технологиями, мы говорим: "Не волнуйтесь. Все будет нормально". Для использования сетей не требуется изощренного ума или сверхъестественных способностей — это скорее вопрос использования языка, который доступен обычным людям.

Эта книга адресована обычным людям, вот почему она рассказывает об использовании Windows Server 2003 и сетей простыми словами. Нет ничего слишком высокопарного, над чем нельзя было бы посмеяться, или чего-то загадочного, что нельзя было бы выразить простым языком. И даже когда нам приходится оперировать техническими терминами, мы предупреждаем вас об этом и стремимся объяснить их как можно понятнее.

Цель этой книги — помочь вам удовлетворить свои потребности. Здесь вы найдете все, что вам требуется знать о Windows Server 2003 и сетях, без необходимости по ходу дела изучать сложные термины или получать ученую степень в области вычислительной техники. Мы действительно хотим помочь вам!

Об этой книге

Структура этой книги такова, что вы можете открыть ее на любой странице и читать как справочное пособие. Части I и II охватывают основы компьютерных сетей: понятия и терминология описаны в части I, проектирование и развертывание сетевого оборудования — в части II. Части III–V посвящены пространному изложению тем, связанных с Windows Server 2003 и сетями. В части III рассматриваются установка и настройка конфигурации системы Windows Server 2003, а в части IV — ее сопровождение и управление. В части V содержатся главы, посвященные борьбе с разнообразными неполадками.

Каждая глава разделена на автономные разделы, каждый из которых связан с основной темой главы. Например, глава, посвященная установке сетевой интерфейсной платы (или адаптера), содержит следующую информацию.

- ✓ Описание адаптера и способа его работы.
- ✓ Различные шины ПК, для которых имеются адаптеры.
- ✓ Как приступить к процессу установки, описав текущую конфигурацию.
- ✓ Как вставить сетевую плату в ПК.
- ✓ Как настроить конфигурацию адаптера после ее установки в ПК.
- ✓ Что делать, если технология Plug-and-Play отказывается работать как следует.
- ✓ Методы борьбы с неполадками, применяемые после того, как первая (вторая) попытка установить адаптер не сработала.

Нет нужды запоминать содержание этой книги. В каждом разделе вы найдете необходимые факты, которые помогут вам легко справиться с сетями, работающими под управлением серверов Windows Server 2003. Однако в некоторых случаях у вас может возникнуть желание работать по книге, чтобы быть уверенным в том, что вы все делаете правильно.

Как читать эту книгу

Поскольку эта книга является справочником, начинайте с того раздела, который вас интересует. Чтобы определить общие области интереса или широкие тематические разделы, вы можете воспользоваться содержанием. Однако предметный указатель, безусловно, — лучший способ отыскать в книге необходимые понятия, родственные темы или конкретные функции, средства и элементы управления Windows 2003.

Если вы никогда не работали с сетями, неплохо полностью прочитать части I и II. Точно так же, если вы не работали с Windows Server 2003, вам было бы полезно прочитать части III и IV. В противном случае начинайте "копать" там, где вам заблагорассудится!

Если вам необходимо ввести что-нибудь с клавиатуры, вы примерно увидите такой текст: ВВЕДИТЕ ЭТО. Предполагается, что вы вводите этот текст с клавиатуры, а затем нажимаете клавишу <Enter>. Поскольку характер ввода может иногда сбить с толку, мы всегда стараемся описать, что именно вы вводите и почему это необходимо.

Время от времени в этой книге предполагается, что вы обращаетесь к справочной системе Windows Server 2003, печатным руководствам, пакету Resource Kit и даже компакт-диску TechNet от Microsoft. И все-таки в большинстве случаев вы найдете все, что вам необходимо знать по конкретной теме, прямо здесь (за исключением некоторых причудливых подробностей, которые в большом числе имеются в Windows Server 2003).

Если некоторую тему, по которой вам требуется знать больше, мы не охватили в этой книге, мы советуем обратиться к книгам серии *...для "чайников"*, опубликованных издательством "Диалектика". Кроме того, в Internet имеется целое море информации, посвященной Windows Server 2003; поиск подобной информации неплохо начать с Web-узла Microsoft `www.microsoft.com/windowsserver2003/default.mspx`.

Глупые предположения

Мы решили выйти из трудного положения и сделали несколько потенциально глупых предположений касательно вас, наш великодушный читатель. У вас есть компьютер, сеть и по крайней мере одна копия Windows Server 2003 (или вы думаете приобрести все это). Вы знаете, что вы желаете делать с этими вещами. Вы даже способны делать многое из этого самостоятельно, если кто-нибудь поможет вам. Цель нашей книги состоит в том, чтобы уменьшить вашу потребность в этом "кто-нибудь", но мы не рекомендуем вам в голос говорить ему об этом — по крайней мере, до тех пор, пока вы закончите читать эту книгу!

Структура книги

Книга разделена на шесть частей, каждая из которых содержит от двух до семи глав. Каждая глава охватывает основную тему и поделена на разделы, в которых рассматривается некоторый конкретный вопрос, касающийся этой темы. Так организована эта книга, но то, как вы станете ее читать — решать вам. Выберите тему, раздел, главу или часть, в которую вы желали бы углубиться или которая соответствует вашим нуждам, и начинайте читать.

Часть t. Закладываем основы сети

В части I рассматриваются сетевые понятия и терминология, включая основы сетевых взаимодействий, а также аппаратное и программное обеспечение, которые заставляют сеть работать. Здесь вы найдете сетевые термины и понятия, такие как клиент, сервер, протокол и топология. Если вы незнакомы с сетями, эта часть как раз придется кстати. Если вы — бывалый "сетевик", можете пропустить эту часть (и часть II).

Часть ll. Подключение оборудования

Часть П охватывает все вопросы, которые вам требуется знать, чтобы создать, или расширить сеть, или просто понять, что в действительности происходит в существующей сети. Она начинается с изложения принципов проектирования и планировки сети и продолжается обсуждением способов установки и настройки конфигурации сетевых адаптеров в ПК. После этого рассматриваются кабельные системы, которые связывают сетевые устройства, и объясняется, каким образом можно соединить несколько сетей. Завершается часть П обзором всех программных компонентов, которые вы, вероятно, можете встретить в сетях, созданных на основе Windows 2003.

Часть III. Серверы, запустить моторы!

В части Ш подробно рассказывается о сервере Windows Server 2003, его установке и конфигурировании. Она охватывает вопросы, связанные установкой и конфигурированием сетевого оборудования применительно к Windows Server 2003. Кроме того, в этой части рассматриваются способы установки и управления серверами и службами печати в сетях на базе Windows 2003, методы обработки TCP/IP-адресов, а также способы установки и управления службами каталогов, доменами и доверительными отношениями в среде, ориентированной на системы Windows 2003. Часть Ш поможет вам понять, как собрать вместе фрагменты сети, используя Windows Server 2003.

Часть IV. Сеть в работе

В части IV рассказывается о том, как поддерживать работу и управлять сетью на базе Windows 2003 после завершения этапа первоначальной установки и настройки конфигурации сети. Она начинается с обсуждения того, как управлять пользователями или группами в сетях на базе Windows 2003, включая детали, касающиеся профилей, правил, а также локальных и глобальных групп. Затем речь идет о способах управления доступом Windows 2003 к файлам NTFS и каталогам, а также о методах управления ресурсами файловой системы, которые доступны в сети и называются совместно используемыми ресурсами.

После того как сетевые пользователи, группы *к* ценные данные определены, перестройка подобных установочных параметров с нуля может доставить немало хлопот. Здесь может пригодиться резервное копирование, так что часть IV касается подробностей резервного копирования и восстановления информации машины, на которой размещена система Windows Server 2003, а также некоторых других аспектов отказоустойчивости. Приводимый после этого обзор принципов и практики сетевой безопасности поможет подготовить ваши данные к защите от случайной утери, а также от возможных атак со стороны хакеров и взломщиков.

Часть V. Выявление и устранение проблем

В части V обращается пристальное внимание на распространенные причины неполадок сетей на базе Windows 2003 и рассматриваются те области, которые первыми могут пасть жертвой неисправностей. Она начинается с обзора некоторых ключевых средств Windows 2003 для выявления неисправностей, а затем приводятся советы и способы борьбы с неполадками в сети на базе Windows Server 2003. Завершается часть V описанием методов борьбы с проблемами использования Active Directory.

Часть VI. Великолепные десятки

Часть VI следует установившейся традиции книг серии *..."для чайников",* каждая из которых содержит часть под названием "Великолепные десятки". Здесь вы найдете перечни сведений, советов и указаний, организованных в виде коротких и удобных глав. Эти вспомогательные сведения будут одинаково полезны и содержательны и предоставляются совершенно бесплатно.

Пиктограммы, используемые в книге

Пиктограммы, используемые в этой книге, отмечают важные (и не столь важные) места в тексте.

Информация, которую важно усвоить, если вы действительно стремитесь *понять,* что происходит в сети или Windows Server 2003.

Ой-ля-ля! Мы сами такие старые, что не можем вспомнить, что означает эта пиктограмма. Может, вам самим следует отметить одну и посмотреть, стоит ли следить за ними!

Эта пиктограмма дает вам знать, что вы вот-вот можете погрязнуть в технических деталях. Мы включили эти сведения, потому что они нравятся нам, и мы вовсе не думаем, что вы должны овладеть ими, чтобы применить к сетям или Windows Server 2003. Если вы стремитесь стать компьютерным фанатом, возможно, вам захочется ее прочитать; если вы уже фанат, может, у вас возникнет желание написать нам о том, что мы упустили, или сообщить другие сведения, которые заслуживают упоминания в книге!

Здесь приведен полезный совет. Мы также используем эту пиктограмму, когда предлагаем идеи, которые, мы надеемся, сделают создание сети или использование Windows Server 2003 более интересным и легким. Например, в тех местах, где мы приводим быстрые клавиши, которые увеличивают продуктивность работы, стоит такая пиктограмма.

Эта пиктограмма означает то, о чем говорит ее название, — очень внимательно относитесь к информации, которая здесь приводится. В девяти случаях из десяти она предупреждает о том, что нельзя делать того, что может иметь плохие или тяжелые последствия, например такие, как случайное стирание всего содержимого жесткого диска.

Куда двигаться дальше

Имея под рукой эту книгу, вы будете готовы бороться с сервером Windows Server 2003 и подключенными к нему сетями. Отыщите тему, откройте нужную страницу, и вы готовы к схватке. Не стесняйтесь делать пометки в книге, пишите на полях, загибайте страницы, делайте все то, от чего тошнит библиотекаря. Самое важное, чтобы вы с толком ее использовали и при ее чтении испытывали удовольствие.

Пожалуйста, загляните на Web-страницу www.dummies.com и не забудьте поделиться с авторами впечатлениями о прочитанном по электронной почте.

Ждем ваших отзывов!

Вы, читатель этой книги, и есть главный ее критик и комментатор. Мы ценим ваше мнение и хотим знать, что было сделано нами правильно, что можно было сделать лучше и что еще вы хотели бы увидеть изданным нами. Нам интересно услышать и любые другие замечания, которые вам хотелось бы высказать в наш адрес.

Мы ждем ваших комментариев и надеемся на них. Вы можете прислать нам бумажное или электронное письмо, либо просто посетить наш Web-сервер и оставить свои замечания там. Одним словом, любым удобным для вас способом дайте нам знать, нравится или нет вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более интересными для вас.

Посылая письмо или сообщение, не забудьте указать название книги и ее авторов, а также ваш обратный адрес. Мы внимательно ознакомимся с вашим мнением и обязательно учтем его при отборе и подготовке к изданию последующих книг. Наши координаты:

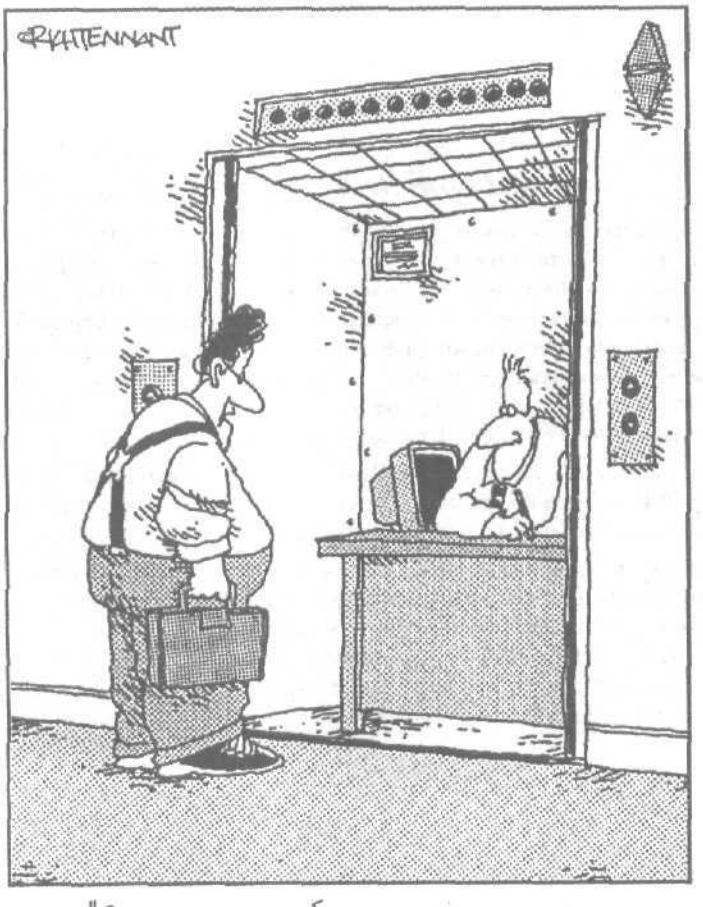
E-mail: info@dialektika.com
WWW: http://www.dialektika.com

Информация для писем из:

России: 115419, Москва, а/я 783
Украины: 03150, Киев, а/я 152

Часть I

Закладываем основы сети



"Это у вас проблемы с постоянным подключением к сети?"

В этой части...

В этой части вы получите основные сведения о локальных сетях (ЛС). Здесь вы найдете ответы на наиболее существенные вопросы: как компьютеры взаимодействуют между собой, почему это взаимодействие заслуживает самого серьезного внимания и что заставляет сеть работать. Мы также раскроем некоторые жизненно важные понятия, включая понятие *протокола*, играющего роль правил "общения", которые компьютеры используют для обмена информацией, и понятие *топологии*, которая описывает способ расположения сетевых коммуникаций.

По ходу дела вы усвоите все основные сетевые термины и понятия, с которыми, возможно, никогда ранее не встречались, но которые вам потребуются для работы с Windows Server 2003.

Материал каждой главы представлен в виде небольших, легких для чтения разделов. Если информация носит сугубо технический характер (большую часть ее можно пропустить, если только вы не заядлый любитель; подобных вещей), на это явно указано в тексте. И все же мы надеемся, что эта информация также окажется полезной для вас — и, может быть, даже заставит улыбнуться.

Глава 1

Создание сети: игра стоит свеч

В этой главе...

- Знакомство с сетевым оборудованием и ПО
- Немного о структуре сети
- Как убедиться в том, что сеть работает
- Совместное использование ресурсов
- Направления развития сетей Windows в новом тысячелетии

Если вам когда-нибудь приходилось говорить по мобильному телефону или следить за телевизионным шоу, то вы пользовались сетью, возможно, даже не подозревая об этом. Большая часть современной мировой инфраструктуры электронных коммуникаций, включая проводную и беспроводную телефонную связь, кабельное и вещательное телевидение, а также Internet, построена на основе сетей.

Для работы сервера Windows Server 2003 также необходима сеть. Поскольку серверы существуют для того, чтобы предоставлять клиентам услуги доступа к файлам, каталогам, Web, обеспечивать печать, безопасность и другие виды услуг, использование Windows Server 2003 без сети подобно использованию телефона, который не включен в розетку. Хотя этот телефон и может представлять определенную ценность как произведение абстрактного искусства, его истинная ценность заключается в том, что он дает вам возможность общаться с другими людьми или службами. То же самое справедливо и для Windows Server 2003.

В этой главе мы познакомим вас с различными компонентами, которые составляют сеть на основе Windows Server 2003, и кратко рассмотрим их работу.

Что такое сеть

Для существования *сети (network)* необходимо наличие хотя бы двух компьютеров, соединенных таким образом, чтобы они могли общаться друг с другом. Для передачи сигналов и данных между компьютерами в большинстве сетей используется электропроводка. Однако для поддержки сетевых соединений используются многие другие виды сетевых сред, включая беспроводные технологии и оптоволоконные кабели. Другими словами, существует много способов попасть из одной точки современной сети в другую!

К числу основных составляющих сети всегда относится некоторое физическое соединение, которое позволяет компьютерам посылать сообщения в среду передачи информации определенного типа, а также "слушать" эту среду. Даже в случае беспроводного канала связи должно существовать физическое соединение компьютеров с антенной или аналогичным устройством, которое позволяет компьютерам транслировать и получать сигналы.

Однако для создания сети одного оборудования недостаточно. Хотя кабели и соединения важны, без программного обеспечения они могут служить, в лучшем случае, просто украшением и будут совершенно бесполезны. В следующих разделах мы более подробно остановимся на оборудовании и ПО, которые заставляют сеть работать.

Без оборудования нет и соединения!

Прежде всего, для создания сети требуется работающее соединение, чтобы дать возможность компьютерам обмениваться информацией друг с другом. *Сетевое оборудование* создает соединение между компьютерами и сетью и образует канал (или среду), который и дает возможность информации перемещаться от отправителя к получателю.

Сетевое оборудование охватывает широкий спектр устройств, многие из которых вы можете обнаружить в своей сети. В первой части этой книги мы поможем вам понять, какую роль играют эти устройства и какие функции выполняют.

С наиболее общей точки зрения компьютерам для взаимодействия в пределах типичной сети необходимо следующее оборудование.

- **Сетевая интерфейсная плата (network interface card** — NIC), или сетевой адаптер, вставляется в компьютер и присоединяется к сетевому кабелю (если используется другая среда передачи данных, то — к этой среде). Он преобразует информационные биты компьютера в идущие по проводу сигналы для исходящего потока данных и преобразует входные сигналы в информационные биты для входящего потока данных.
- **Соединительные разъемы,** или **коннекторы (connectors)** позволяют подключить сетевой адаптер к сетевой среде. Для беспроводных сред коннекторы подключают антенны или другие передающие устройства к сетевому адаптеру. Можно сказать, что коннекторы собирают отдельные компоненты сетевого оборудования в единое целое.
- **Кабели** транспортируют сигналы от передатчика к получателю; при этом в электрических кабелях используются электрические сигналы, а в оптоволоконных — световые импульсы. В случае беспроводной среды канал связи образуется с помощью радиоволн, используемых для передачи информации между отправителями и получателями.
- **Дополнительные сетевые устройства** используются для создания более масштабных и сложных сетей. Диапазон этих устройств изменяется от простых концентраторов, используемых для звездообразных сетей (подробно об этом рассказывается в главах 4 и 7), до повторителей, используемых для связывания отдельных сегментов кабеля, а также мостов, маршрутизаторов и шлюзов (детальная информация представлена в главе 7). Оборудование играет важную роль в создании сетей. Оно не только позволяет подключать компьютеры к сети, но и дает возможность объединить несколько сетей и управлять потоками данных из одной сети в другую.

О требованиях к сети

- Все требования к созданию сети сводятся к наличию следующих трех основных составляющих сети; соединений, протоколов связи и сетевых служб.
- **Соединения** включают оборудование, необходимое для подключения компьютеров к сети, з также кабели (называемые сетевой средой), которые перегоняют сообщения между компьютерами. Устройство, которое подключает компьютер к сети, называется ***сетевым интерфейсом.*** В большинстве случаев для подключения ПК к сети требуется вставить плату адаптера, называемую ***сетевой интерфейсной платой.*** Без физического соединения компьютер не сможет использовать сеть.
- Сетевые протоколы определяют правила, которым должны следовать компьютеры при обмене и интерпретации информации, Поскольку каждый компьютер может функционировать под управлением ПО, отличного от ПО других компьютеров, компьютерам объединенным в сеть, требуется общий язык, который позволил бы им обмениваться сообщениями и данными. Без совместно используемых средств общения компьютеры не смогут обмениваться данными, даже несмотря на то, что они могут пользоваться общей сетевой средой.

- ✓ **Службы** предоставляют услуги, которые компьютеры могут оказывать друг другу, включая отправку и получение файлов, обмен сообщениями, задания на печать и т.п. Другими словами, сетевые услуги — это основная тема общения компьютеров. Если компьютеры не могут оказывать друг другу услуги в пределах сети, они не способны ни отвечать на запросы от других компьютеров, ни требовать выполнения какой-либо работы для себя.

Без ПО сеть не станет работать!

Благодаря программному обеспечению компьютеры получают доступ к оборудованию и возможность использовать его, независимо от того, применяется ли это оборудование для реализации сетевых функций или предназначено для чего-то другого.

Теперь вам должно быть понятно, что оборудование обеспечивает необходимые соединения, которые делают возможным создание сети, а ПО поддерживает взаимодействие и услуги, необходимые для доступа к оборудованию и сети, к которой это оборудование подключено.

Работа современных компьютерных сетей поддерживается многими различными видами ПО. Это ПО включает специализированные программы, называемые *драйверами устройств (device driver)*, которые позволяют компьютерам обращаться к сетевому интерфейсу и обмениваться данными с ним. Набор программных средств включает также приложения, которые могут с равным успехом обращаться к данным на локальном компьютере или на сервере ц пределах всей сети. ПО включает также целую группу других средств, которые занимают промежуток между драйверами и приложениями.

В этой книге мы расскажем, как распознавать различные компоненты ПО, участвующие в работе сети, и как наилучшим образом настраивать конфигурацию этого ПО для работы с Windows Server 2003.

Исследуем возможности вашей сети

Если вы исследуете обычную сеть, то узнаете, как много различных типов оборудования и связанного с ним разнообразного ПО используется в ней. Если вы составите реестр всех компонентов сети, то сможете использовать эти данные для того, чтобы понять, что подключено к вашей сети и какие функции выполняют в ней различные устройства.

Инфраструктура, делающая возможным организацию сети, образована оборудованием, которое привязывает компьютеры к сети кабелями или другой сетевой средой, которая переправляет информацию между компьютерами, а также аппаратным и программным обеспечением, используемым для создания и управления сетью. Вы также можете присовокупить сюда скопление соединений, кабелей, адаптеров и другого *"скрепляющего"* оборудования, поскольку эти элементы связывают компьютеры в работающую сеть.

Три ступени сетевой организации

Сетевое ПО подразделяется на три категории; "главный узел терминал", "клиент/сервер" и "соединение равноправных узлов". Каждая из категорий отражает определенный тип сетевого взаимодействия,

- ✓ **Сети типа главный узел-терминал** базируются на устаревшей сетевой модели, даже если они не используют устаревшее оборудование. В первоначальной версии этой сети пользователи обращались к информации посредством устройства, которое называлось ***терминалом*** и состояло из экрана, клавиатуры и сетевого соединения. Все ПО функционировало на мощном компьютере, называемом главным ***узлом*, или *хостом* машиной** *(host)*, который располагался в некотором месте сети.

Единственное, на что было способно это непритязательное устройство, — это обеспечение пользователям доступа к удаленным данным и приложениям (вот почему подобное устройство также известно под названием **неинтеллектуальный терминал**, или **терминал ввода-вывода** *(dumb terminal)*). *В* более современных версиях ПК могут работать в качестве терминалов с помощью ***ПО эмуляции терминала***, которое ПК использует для доступа к главному узлу, При этом ПК по-прежнему обеспечивает некоторые локальные интеллектуальные функции и доступ к локальному ПО текстовых процессоров, электронных таблиц и т.д. На самом деле возможности сети "главный узел терминал" поддерживаются Windows Server 2003 с помощью специальной программы обслуживания терминалов — ***Terminal Server***

- ✓ **Сеть с архитектурой** клиент/сервер состоит из набора интеллектуальных машин. Одна или несколько из этих машин работают в качестве сервера и оснащены памятью большого объема, мощным процессором и сетевым ПО, так что они могут обрабатывать запросы от других машин. Остальные машины, которые взаимодействуют с сервером, называются клиентами. Иногда сети "клиент/сервер" называют также ***сетями* на основе *сервера,*** чтобы подчеркнуть ведущую роль сервера. Windows Server 2003 обеспечивает базис для сети "клиент/сервер", которая является темой настоящей книги. Помимо Windows Server 2003, аналогичную роль в современных сетях также играют серверы ***NetWare*** от Novell и ***UNIX.***
- ✓ **В сети с равноправными** узлами (или одноранговой сети) любая машина, которая может быть клиентом, может также выступать в роли сервера. В отличие от сетей "клиент/сервер" в качестве сервера не выделяется какая-либо специализированная машина. 8 одноранговой сети все машины обладают более-менее равными возможностями, а также предлагают приблизительно одинаковые услуги. Если вы пользуетесь встроенными сетевыми возможностями, имеющимися в таких ОС, как ***Windows XP Professional***, *Windows* ***2000 Professional, Windows NT Workstation,*** *Windows* ***95,*** *Windows* ***98, Windows Me,*** вы работаете именно с этим типом сетевого ПО.

Каждому - по рабочей станции!

Одно из главных преимуществ использования сети заключается в том, что она берет на себя функции, которые вы выполняете с помощью своей настольной системы, — готовы поспорить, что вы обычно называете это "работой", — и позволяет вам выполнять их более эффективно за счет взаимодействия с удаленными ресурсами и данными. Это значит, что вы можете обращаться к файлам на сервере так, будто они представляют собой часть вашего собственного диска, отправлять задание принтеру в любую точку сети так, будто он подключен непосредственно к вашей машине, и т.д. Совместное использование ресурсов остается самым превозносимым преимуществом сетей, поскольку они соединяют ваш настольный компьютер с хранилищами файлов, принтерами, приложениями и информационными ресурсами, которые в противном случае были бы недоступными или слишком дорогими для того, чтобы хранить их на каждом настольном компьютере.

В мире компьютерных сетей термины *сетевой клиент (network client), настольный компьютер (desktop computer)* и *рабочая станция (workstation)* используются в некоторой степени как синонимы. Неважно, как вы называете их, это те машины, на которых пользователи выполняют основную массу своей работы (и, возможно, в редкие минуты позволяют себе поиграть).

Рабочим столом (desktop) называют область экрана компьютера, которая отображает пиктограммы и "обои".

Одна из главных причин, побуждающих организации к созданию сетей, — стремление связать между собой все рабочие станции, независимо от того, работают ли они под управлением операционной системы DOS, Windows, UNIX, Linux или Macintosh, так, чтобы они могли взаимодействовать и совместно использовать ресурсы. К ресурсам, совместно используемым рабочими станциями, относятся большие массивы дисковой памяти, дорогостоящие

цветные и лазерные принтеры, дисководы с автоматической сменой компакт-дисков и высокоскоростные Internet-соединения (все эти ресурсы оказались бы слишком дорогостоящими при подключении к каждой настольной машине).

Для большинства сетей соотношение количества настольных машин и пользователей весьма близко к значению "один к одному. Другими словами, каждый пользователь обладает доступом к рабочей станции, подключенной к сети, даже если этот пользователь не единственный, кто работает на этой машине. Поскольку эти рабочие станции служат источниками запросов на обслуживание, такие машины получили название сетевых клиентов, или *клиентов*.

Когда вы называете такую машину *рабочей станцией*, вы подчеркиваете ее способность поддерживать отдельного пользователя более-менее независимо. Когда вы называете такую машину *клиентом,* вы акцентируете внимание на ее подключении к сети. Как бы вы ее назвали, это машина, которая стоит на вашем столе и подключена к сети.

Сервер всегда к вашим услугам

Под сетью понимают, прежде всего, получение доступа к разделяемым ресурсам. Поскольку сеть бесполезна до тех пор, пока вы не сможете с ними работать, именно доступ к ресурсам и составляет сущность сети.

В современных сетях возможности, необходимые для получения доступа к ресурсам и выполнения работ, обеспечивают серверы. Например, когда вы отправляете задание на печать на сетевой принтер, вы можете предполагать, что где-нибудь в фоновом режиме сервер печати обрабатывает задание. Аналогично, когда вы запрашиваете файл с сетевого диска, в "игру вступает" файловый сервер. Когда вы любопытствуете, что же там в сетевом каталоге (вы угадали!), вы "общаетесь" с сервером каталогов. Для каждой услуги определенный тип сервера обрабатывает и отвечает на запрос. Иногда один сервер обеспечивает несколько видов услуг, в других случаях сервер обеспечивает только одну услугу.

Компьютеры, которые предоставляют услуги клиентам, обычно называются *серверами*. Работа сервера состоит в том, чтобы "прислушиваться", не поступил ли от клиента запрос на услугу или услуги, которые он предоставляет, и удовлетворять любые допустимые запросы на обслуживание. На самом деле определение допустимости запросов составляет важную часть обязанностей сервера — вы не можете позволить, чтобы кто угодно мог распечатать информацию о заработках любого сотрудника вашей компании только потому, что пользователь обратился к серверу печати с подобным запросом. Вам требуется, чтобы сервер проверил, что Бобу *разрешен* доступ к этому файлу, прежде, чем позволить ему напечатать его! В последующих главах вы узнаете больше о подобных проверках и других важных требованиях, которым должен удовлетворять сервер, чтобы обслуживать клиентов.

Сетевые магистрали

Между компьютером, которому требуется услуга, и компьютером, задача которого — удовлетворить это требование, должен существовать общий путь. Подобно тому, как вам требуется автомагистраль, чтобы доехать из одного города в другой, вам требуется "сетевая магистраль", по которой компьютер может отправлять и получать данные. Применительно к сети — это функция среды, которая связывает воедино различные ее фрагменты.

Оглянитесь вокруг и присмотритесь к типам кабелей и соединений, используемых в вашей сети. Вникните в ее структуру так, чтобы вы могли сказать, какие магистрали используют пользователи — от "боковых дорожек", которыми пользуются только ребята из отделов работы с клиентами и доставки, до "главной дороги", которую используют все пользователи.

Когда вы поймете, как все эти фрагменты совмещаются — рабочие станции, серверы и среда, — вы получите достаточно полное представление о вашей сети. На рис. 1.1 изображена схема простой сети, на которой показаны эти исключительно физические элементы сети.

Обратите внимание, что клиенты (настольные машины) превосходят численно серверы, а среда объединяет эти компоненты вместе. Сеть подчиняется закону спроса и предложения, так что, чем больше у вас клиентов, тем больше серверов (или более мощных серверов) вам потребуется — и тем большая работа будет сделана!

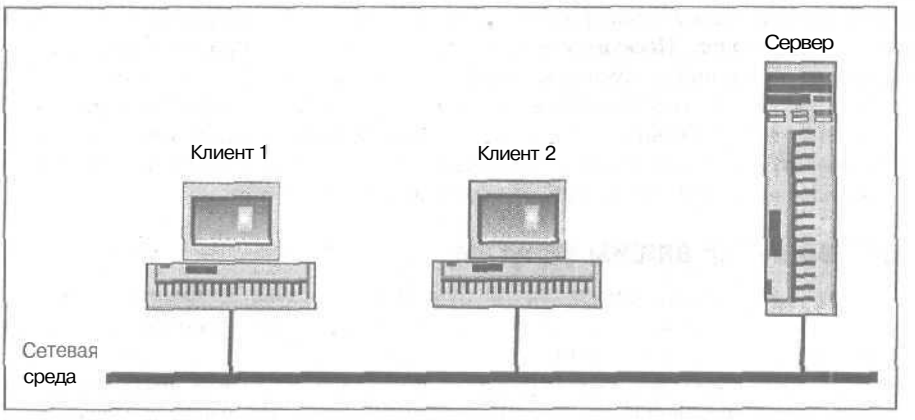


Рис. 1.1. Типичная сеть с клиентами, сервером и инфраструктурой (сетевой средой)

Что значит "работающая сеть"

Понять, действительно ли сеть функционирует, одновременно и легко, и трудно, и большинство наблюдателей, включая новичков и экспертов, сходятся во мнении, что сказать, когда сеть *не работает,* легче, чем сказать, когда она работает! Клиент должен знать, как запросить обслуживание у сети, и должен точно сформулировать, что именно ему требуется. Также сервер должен знать, как распознать и оценить входящие запросы на его услуги и как соответствующим образом ответить. Только тогда сеть, может быть, будет работать правильно.

Понять, как работает этот непрерывный поток запросов и ответов, значит детальнее рассмотреть, как клиент формулирует свои запросы и как серверы удовлетворяют их. В следующих разделах мы изучим механизм этого взаимообмена.

Начало игры: как спросить нужное "блюдо"

Чтобы знать, как запросить ту или иную сетевую услугу, необходимо иметь возможность различать, что доступно локально на клиентской машине и что можно получить в удаленном режиме из сети. Умение определить, какой характер — локальный или удаленный — носит запрашиваемый ресурс, служит ключом к корректной работе с сетевым доступом. Эта функция определения возлагается на специальное ПО, которое обрабатывает задание в фоновом режиме, так что пользователю нет нужды знать об этих различиях.

Главная управляющая программа компьютера называется *операционной системой (ОС),* поскольку она определяет программную среду, которая позволяет компьютеру функционировать (т.е. производить операции) и выполнять приложения и программы системного обслуживания, позволяющие получить на машине некоторые результаты. Большинство современных операционных систем включает встроенные сетевые возможности, расширяющие их контроль над локальными ресурсами и устройствами.

Некоторые современные операционные системы, которые создают сетевую серверную среду, можно назвать *сетевыми операционными системами.* Их встроенные сетевые воз-

можности включают набор сетевых услуг как неотъемлемую часть базовой операционной системы. Windows Server 2003 определенно отвечает этим требованиям, поскольку предоставляет широкий спектр мощных и гибких сетевых возможностей.

Новая ОС Windows Server 2003 "понимает" разницу между локальными и сетевыми ресурсами. То же справедливо и для большинства современных операционных систем, включая Windows XP Professional, Windows 2000 Server и Windows 2000 Professional, Windows NT Server и Windows NT Workstation, Windows 9x, ОС Macintosh, а также для старой, испытанной (но по-прежнему современной) ОС UNIX.

В операционных системах Windows Server 2003, Windows XP Professional, Windows 2000, Windows NT, Windows *9x,* Macintosh и UNIX, а также в расширениях DOS и Windows *3x* существует специальный программный компонент, известный как *редиректор* (*redirector*), который при обращении пользователей или приложений к ресурсам следит за тем, какие из них являются локальными, а какие удаленными. Редиректор принимает исходные запросы на обслуживание и отправляет те из них, которые не могут быть удовлетворены локально, в некоторый узел сети соответствующему поставщику услуг (другими словами — соответствующему серверу). Таким образом, если вы запрашиваете файл, расположенный где-то в сети на сервере, редиректор передаст ваш запрос той машине и позаботится о том, чтобы результат этого запроса был доставлен правильно.

Что сегодня в меню

Чтобы пользоваться сетевыми услугами, компьютер должен знать, как их запросить. Это дело специальной программы — *запросчика (requester).* Однако знать, что запрашивать, не менее важно, чем знать, как запрашивать. В большинстве случаев приложение поставляет необходимую информацию о сетевой услуге, к которой оно желает получить доступ, либо посредством информации поставляемой через запросчика, либо за счет сведений, которыми располагает непосредственно само приложение.

Хорошим примером приложений, обладающих развитыми встроенными сетевыми возможностями, могут служит клиенты электронной почты и Web-броузеры. С другой стороны, средства доступа к файлам наподобие Windows Explorer, My Computer, My Documents, когда им необходимо получить представление о разделяемых файлах и принтерах (и доступ к ним), расположенных на различных узлах сети, полагаются на редиректор.

Пожалуйста, обратите внимание на то, что приложения со встроенными возможностями сетевого доступа обеспечивают *прозрачный* (*transparent*) доступ к сетевым услугам, поскольку приложение знает, как запрашивать услуги и что запрашивать с точки зрения пользователя. Программисты разрабатывают подобные компьютерные приложения именно как "прозрачные", чтобы с ними можно было работать по поговорке "с глаз долой — из сердца вон"; таким образом, пользователи остаются в блаженном неведении в отношении всех этих обременительных подробностей и мелочей. Однако программы управления файлами, принтерами и другие средства, обладающие доступом как к локальным, так и к удаленным ресурсам, требуют от пользователей явного указания различий между первыми и вторыми. Фактически подобные средства обычно заставляют пользователей явно и прямо запрашивать доступ к удаленным ресурсам.

Необходимость в непосредственном знании характера услуг, предоставляемых сетью, все в большей степени исчезает. Это связано с тем, что все версии Windows Server 2003 поддерживают набор служб каталогов для учета и описания услуг, которые сеть может предоставить ее пользователям. Аналогично, Windows Server 2003 поддерживает распределенную файловую систему (Distributed File System — DFS), за счет которой каталоги на многих машинах по

всей сети выглядят для пользователей как единый сетевой диск. Таким образом, пользователям нет нужды знать, где расположены отдельные файлы и папки.

Подобный развитой механизм как никогда ранее облегчает пользователям неявный запрос ресурсов и доступ к ним, избавляя их от необходимости знать, как запрашивать эти ресурсы и точно определять место их расположения. Тем не менее, если вам требуется извлечь максимум пользы из сетевых возможностей Windows Server 2003, вам все же придется вникнуть в некоторые подробности, касающиеся этих аспектов работы с сетью.

Совместно используемые ресурсы

Механизмы формирования запросов на ресурсы зависят от наличия доступа к подходящим программным средствам, позволяющим определить, когда возникает необходимость в сетевых запросах. ПО доставляет запрос серверу, задача которого заключается в прослушивании подобных запросов и удовлетворении всех тех из них, которые являются правомерными. В конечном итоге задача сервера состоит в том, чтобы дать доступ к ресурсам всем пользователям, имеющим на это право. Реализация этой функции делает возможным совместное использование ресурсов и помогает объяснить наиболее существенный выигрыш от использования сети, а именно: обеспечение единообразного, согласованного способа получения безопасного и управляемого доступа к файлам, принтерам, сканерам, данным, приложениям и т.д. со стороны многочисленных пользователей.

Секрет в разделении ресурсов состоит в изыскании способа, который бы гарантировал каждому возможность получения доступа к совместно используемым ресурсам. Например, для доступа к службе печати необходимо, чтобы входящие задания на печать сохранялись во временной области памяти до тех пор, пока не наступит их очередь вывода на принтер. Таким образом, разделение принтера означает не только обеспечение доступа собственно к самому устройству, но также слежение за тем, что поступает на вход устройства, и обеспечение места, где могут разместиться ожидающие задания, а иногда и уведомление пользователей об успешном завершении задания на печать. Все эти механизмы облегчают выполнение разделяемых заданий и объясняют, почему серверы играют такую важную роль в любой сети.

Поскольку серверы объединяют услуги и данные в пределах одной машины, они выступают в качестве естественного центра контроля и сопровождения для многих важных устройств, служб и данных в сети, к которым, безусловно, стремятся получить доступ многие сетевые пользователи.

Тенденции в развитии сетей Windows

Компания Microsoft стремительно вступает в новую эру, которая отличается небывалой доселе интеграцией локальных сетей и доступа к Internet. Windows Server 2003 — следующий шаг Microsoft на пути к достижению цели создания сквозных сетевых структур, которые дадут возможность компаниям и отдельным пользователям легко, эффективно и безопасно общаться посредством электронных коммуникаций. Windows Server 2003 построена на технологии, базирующейся на Windows 2000, которая, в свою очередь, основана на технологии, заимствованной из Windows NT. Семейство продуктов Windows Server 2003 охватывает несколько типов серверов, включая следующие их разновидности.

- ✓ Windows Server 2003, Web Edition. Серверная система, оптимизированная для Web-служб и Web-узлов. Эта версия поддерживает до четырех процессоров и 2 Гбайт оперативной памяти (ОП) на компьютер.

- ✓ **Windows Server 2003, Standard Edition.** Сервер, разработанный взамен сервера Windows 2000 Server. Он может использоваться в качестве рядового сервера или контроллера домена для сетей небольших и средних размеров. Сервер Standard Edition поддерживает до четырех процессоров и 4 Гбайт ОП на компьютер. Он также рассматривается в этой книге.
- ✓ **Windows Server 2003, Enterprise Edition.** Эту версию можно рассматривать как Windows Server 2003, Standard Edition со множеством всяких "прибамбасов". Эта "навороченная" версия позволяет использовать до восьми ЦП (процессоров) и до 32 Гбайт ОП на одном сервере (что помогает увеличить производительность). Windows Server 2003, Standard Edition поддерживает объединение в кластеры до восьми узлов (соединение двух и более компьютеров таким образом, что все они разделяют общую рабочую нагрузку для поддержки одного масштабного приложения или сетевой службы).
- ✓ **Windows Server 2003, Datacenter Edition.** Это мощная операционная система Windows, которая поддерживает даже больше ЦП и ОП, чем Windows Server 2003, Enterprise Edition (до 64 ЦП и 64 Гбайт ОП)). Она обладает такими же функциональными возможностями, что и версия Enterprise Edition, и некоторыми дополнительными. Windows Server 2003, Datacenter Edition может одновременно поддерживать в определенных ситуациях больше 10000 пользователей и кластеры, содержащие до восьми узлов.

Существуют также версии *Windows Server 2003, Enterprise Edition* и *Windows Server 2003, Datacenter Edition,* разработанные для 64-разрядного процессора Itanium компании Intel.

Хотя эти версии и отличаются, в них больше общего, чем различий. Поэтому эта книга поможет вам овладеть основами знаний, касающихся всех типов продуктов семейства Windows Server 2003.

Основываясь на возможностях Windows Server 2003, мы можем говорить о следующих тенденциях в развитии сетей Windows, которые могут проявиться в новом тысячелетии.

- ✓ **Использование Active Directory.** *Active Directory* — это название службы каталогов Microsoft, поддерживаемой Windows Server 2003. Служба Active Directory облегчает пользователям идентификацию и доступ к сетевым ресурсам, а приложениям — непосредственное и автоматическое использование подобных ресурсов. В настоящее время вы можете не видеть достаточных оснований в пользу подобной возможности, но в ближайшем будущем она изменит наш подход к использованию Windows.
- ✓ **Доступ к динамической дисковой памяти.** Windows Server 2003 поддерживает различные развитые технологии разделения каталогов. Динамическая дисковая память дает возможность сетевым администраторам определять наборы файлов и каталогов, собранных с нескольких серверов в пределах сети, и представлять их пользователям так, будто файлы и каталоги расположены на едином сетевом диске. Это облегчает создание, идентификацию и доступ к наборам совместно используемых файлов.
- ✓ **Службы согласованного именования.** Отчасти задача определения местонахождения ресурсов в сети заключается в определении их имен (или способа их нахождения). Windows Server 2003 использует единый усовершенствованный метод для перевода понятных человеку имен сетевых ресурсов в сетевые адреса, понятные компьютеру. Это значительно упрощает управление сетевыми ресурсами и взаимодействие с ними.

- ✓ Web-ориентированная консоль управления. В Windows Server 2003 консоль MMC (Microsoft Management Console — консоль управления Microsoft) играет роль хоста в управлении средствами (называемыми интегрируемыми MMC-средствами) для всех системных служб, ресурсов и функциональных возможностей. Эта консоль упрощает интерфейс Windows Server 2003, а ее многочисленные функции визуально более согласованны и, таким образом, более просты в изучении и управлении. Фактически эта функциональность работает на любом компьютере, оснащенном подходящим Web-броузером (и обладающем административными правами).
- ✓ Упрощенная разработка и доставка содержимого Web-узлов. Одна из главных целей функционирования семейства серверов Windows Server 2003 состоит в том, чтобы предоставлять в распоряжение конечных пользователей (т.е. заказчиков) мощные, приносящие высокую прибыль службы и приложения, причем осуществлять это наиболее эффективным способом. Посредством использования оптимизированных средств для Web, новых языков программирования и архитектур разработки Web-контента (т.е. содержимого Web-узлов) Windows Server 2003 призван революционизировать создание, развертывание и сопровождение корпоративных Web-узлов.

Если предположить использование всех этих возможностей, становятся очевидными тенденции развития сетей Windows.

- ✓ Более легкий и непосредственный доступ к сетевым ресурсам.
- ✓ Упрощенное администрирование и управление этими ресурсами.
- ✓ Более развитые средства и технологии описания, предоставления и контроля сетевых ресурсов.

Так воспользуйтесь этими возможностями!

Глава 2

Сеть с архитектурой "клиент/сервер"

В этой главе...

- Запрос на обслуживание
- Предоставление услуг
- Диалог клиента с сервером
- Лучшая сеть — "родная"
- Добавление расширенных сетевых возможностей
- Знакомство с сетью Microsoft (и ее альтернативами)
- Управление сетевым доступом
- Использование сетевых служб Windows Server 2003

Для большинства приложений работа с Windows Server 2003 в сетевой среде предполагает использование модели "клиент/сервер". Чтобы помочь вам понять эту сетевую модель, которая как нельзя лучше объясняет необходимость такой системы, как Windows Server 2003, мы подробно рассмотрим в этой главе модель "клиент/сервер". Вы узнаете много нового о функциональных возможностях и сетевых службах, которые составляют сущность работы сети "клиент/сервер", а также о различных способах взаимодействия клиентов и серверов в подобной сети.

Клиенты просят об услугах

В главе 1 мы объяснили, что клиенты просят о предоставлении услуг и что для работы каждого компьютера в сети необходимо аппаратное и программное обеспечение. В этой главе мы более подробно рассмотрим различные компоненты и составляющие, участвующие во взаимодействии клиента и сервера, чтобы помочь вам понять, что происходит, когда клиент просит сервер обслужить его.

В самом общем случае клиент должен обладать сетевым соединением, позволяющим передавать запрос на обслуживание. Также клиент должен быть оснащен надлежащим ПО, установленным для того, чтобы сформировать четкий запрос и передать его в сеть, где сервер может обнаружить подобный запрос и ответить на него.

Создание соединения

Для формирования запроса на обслуживание клиент должен быть оснащен следующими аппаратными средствами.

- Сетевая **интерфейсная** плата (network interface card — **NIC).** Плата сетевого интерфейса (называемая также сетевым адаптером или сетевой картой) дает возможность компьютеру взаимодействовать с сетью. Перед тем как сетевой адаптер сможет передавать сигналы в сетевую среду и получать сигналы из нее, вы должны настроить его конфигурацию.

- ✓ **Физическое соединение.** Канал между компьютером и сетью должен работать надлежащим образом. Это значит, что клиенты могут передавать исходящие сигналы и получать входящие посредством их сетевого соединения. Аналогично, сама сетевая кабельная система, известная также как сетевая среда, должна быть соответствующим образом сконфигурирована и коммутирована, чтобы сигналы могли проходить от отправителя к получателю.

Рассмотренное выше оборудование касается той части простой трехкомпонентной модели сети, которая относится к соединениям, и требует, помимо исправно работающих соединений, наличия средств коммуникации и сетевых служб.

ПО использует соединение

ПО на клиентском компьютере работает с сообщениями и услугами, необходимыми для функционирования сети. Ниже приведен список ПО, которое вы, как правило, можете обнаружить на подключенном к сети клиентском компьютере, начиная с уровня оборудования (или, точнее говоря, с уровня ПО, наиболее близко соприкасающегося с оборудованием) и заканчивая приложениями, которые запрашивают сетевые услуги.

- ✓ **Сетевой драйвер.** Специальное ПО, которое позволяет компьютеру посылать данные из центрального процессора (ЦП) сетевому адаптеру, когда исходящее сообщение готово к отправке. Когда приходит входящее сообщение, сетевой драйвер также переправляет ЦП запрос, требующий немедленной реакции (называемый *прерыванием* (*interrupt*)). Можно сказать, что драйвер дает возможность ПК общаться с сетевым адаптером, который взаимодействует с сетью.
- ✓ **Стек протоколов.** Набор коммуникационного ПО, которое обеспечивает своего рода "общепонятный язык", необходимый для успешной работы сети. Стек протоколов обусловливает предполагаемый формат сетевых сообщений и определяет набор правил по интерпретации их содержимого. Для взаимодействия двум компьютерам необходимо использовать один и тот же стек протоколов. Более основательно мы рассмотрим стеки протоколов в главе 3.
- ✓ **Редиректор.** Редиректор, или эквивалентное ПО, выдает запросы для удаленных ресурсов или услуг стеку протоколов и получает входящие ответы от стека протоколов. Когда редиректор функционирует в фоновом режиме, приложения не нуждаются в явной осведомленности о состоянии сети, поскольку с сетевыми соединениями управляется редиректор.
- ✓ **Приложения, осведомленные о состоянии сети.** Приложения, осведомленные о состоянии сети, распознают, может ли запрос на обслуживание быть удовлетворен локально или должен быть удовлетворен за счет удаленного обслуживания. В последнем случае редиректор может присутствовать, но он не обязательно может управляться с определенными типами сетевых служб (например, такими как электронная почта или доступ к Web-страницам). Однако редиректор может управляться с другими типами сетевых служб, такими как предоставление доступа к файлам, расположенным где-то в сети, которые прилагаются в качестве дополнения к сообщениям электронной почты. В подобном случае редиректор захватывает копию этого файла в любом месте сети и присоединяет его к исходящему сообщению электронной почты.

Когда клиент делает запрос на ресурс или услугу, которые требуют доступа к сети, либо приложение (если оно осведомлено о состоянии сети), либо редиректор (если приложение не знает состояния сети) формирует формальный запрос на удаленную услугу. Удовлетворение

запроса может вызывать передачу небольшого объема данных (как, например, в случае запроса на содержимое каталога для машины, расположенной в определенном месте сети). Однако иногда может потребоваться передача больших объемов данных (как, например, в случае отправки на печать большого файла или копирования большого файла с клиентской машины на сервер).

Запрос транспортируется через стек протоколов, которым сообща пользуются клиент и сервер. Для коротких запросов небольшая порция коротких сообщений проходит от клиента и затем вновь собирается и обрабатывается сервером. При передаче больших объемов информации клиент разбивает файл на сотни или тысячи небольших информационных пакетов, каждый из которых доставляется по сети отдельно и затем собирается на принимающей стороне.

Стек протоколов приказывает сетевому драйверу отправить небольшие пакеты данных (называемые *кадрами (frame)* или *пакетами* (*packet*))с компьютера через сетевой адаптер и далее по сети к предполагаемому получателю (серверу). На принимающем конце те же действия происходят в обратном порядке, за исключением одного дополнительного обстоятельства, о котором речь пойдет в следующем разделе.

Серверы предоставляют услуги

В предыдущем разделе вы узнали о том, что клиенты просят об услугах, а серверы предоставляют их. Обработка запроса на стороне сервера в действительности означает, что специальный крошечный компонент ПО, называемый *процессом-слушателем (listener process),* непрерывно функционирует на сервере и прослушивает сеть на предмет запросов на определенную услугу. Когда приходит запрос, процесс-слушатель обрабатывает его как можно быстрее.

Сервер пробирается сквозь лабиринт запросов

Обычно в большинстве операционных систем, включая Windows Server 2003, происходит следующее: процесс-слушатель распознает приход запроса. Процесс-слушатель проверяет идентичность и ассоциированные полномочия клиента, и если клиент оказывается тем, за кого себя выдает, и обладает надлежащим разрешением на получение услуги, процесс-слушатель передает запрос на обслуживание. Он осуществляет это с помощью запуска временного процесса (на языке Windows называемого *потоком выполняемых задач* (*execution thread);* его можно представить себе как очень маленькую программу), который существует ровно столько, сколько требуется, чтобы справиться с некоторым обслуживанием, запрашиваемым клиентом, — после чего временный процесс исчезает. Например, запрос на определенный файл на сервере приводит к созданию временного процесса, который существует ровно столько, сколько необходимо, чтобы скопировать запрашиваемый файл в пределах сети. Как только копирование завершено, временный процесс перестает существовать!

Использование процесса-слушателя для создания кратковременных потоков выполняемых задач позволяет серверу справиться с большим количеством запросов, поскольку процесс-слушатель никогда не занят надолго обработкой отдельных запросов. Как только процесс-слушатель создаст поток для обработки одного запроса, он проверяет наличие других ожидающих запросов и о мере необходимости обрабатывает их; в противном случае процесс-слушатель возвращается к прослушиванию вновь поступающих запросов. Обычно сервер располагает одним или несколькими процессами-слушателями для каждого вида услуг, которые поддерживает сервер.

Серверы — это программы, управляемые запросами. Это значит, что их задача заключается в том, чтобы отвечать на запросы клиентов на обслуживание. Сервер редко бывает инициатором действий. Этот "реактивный" образ действий сервера помогает объяснить, почему модель "клиент/сервер" также известна как архитектура *запрос-ответ* или *запрос-реакция*, которая отличается тем, что клиент формирует запрос, а сервер отвечает или реагирует на него.

В отличие от необходимого процесса-слушателя и набора сервисных приложений, которые фактически осуществляют обслуживание, серверу требуются те же компоненты аппаратного обеспечения, что и клиенту. Серверу требуется одна или несколько плат адаптера с работающим сетевым соединением, чтобы дать возможность данным приходить и уходить с сервера.

На стороне сервера — аналогичное ПО

С точки зрения ПО серверу также требуются следующие элементы, позволяющие охватить обслуживанием всю сеть.

- ✓ **Сетевые драйверы** дают возможность серверу взаимодействовать с сетевым адаптером. Это ПО скрытно работает в фоновом режиме и существует только для того, чтобы связать компьютер с адаптером.
- ✓ **Стеки протоколов** отправляют и получают сообщения в пределах сети. Это ПО также скрытно работает в фоновом режиме и служит языком общения, понятным также клиентам, который используется при транспортировании информации по сети.
- ✓ **Сервисные приложения** реагируют на запросы по обслуживанию и формируют ответы на них. Это ПО функционирует в фоновом режиме и выполняет полезную работу. Сервисное приложение включает процесс-слушатель, временные потоки выполняемых задач и некоторый тип конфигурационной или управляющей консоли, так что его по необходимости можно установить, сконфигурировать и изменить. К типичным сервисным приложениям относятся службы каталогов (Active Directory), процессоры баз данных (SQL Server Oracle) и почтовые серверы (Exchange).

Большая часть (если не все) ПО, расположенная на сервере, осведомлена о состоянии сети, поскольку доставка информации по сети является главной функцией серверов.

Расшифровка диалога клиента с сервером

Вас может удивить то, из **каких** шагов состоит диалог между клиентом и сервером. Исследование точного содержимого подобного обмена сообщениями вряд ли принесет вам слишком много пользы. Тем не менее приведенная ниже последовательность действий представляет собой типичный запрос на печать файла на сетевом принтере (и по необходимости посредством сервера печати) из программы обработки электронных таблиц.

1. Пользователь запрашивает услугу печати в программе обработки электронных таблиц, щелкнув на пиктограмме принтера или выбрав команду File⇨Print (Файл⇨Печать). Предположим, что сетевой принтер установлен в качестве выбираемого ло умолчанию принтера для назначенного задания на печать.
2. Программа обработки электронных таблиц форматирует электронную таблицу, а затем создает соответствующий файл печати. Файл печати включает текст и графику, которые составляют содержимое файла. Он также включает инструкции, которые указы-

вают, как (шрифт полужирный, курсив и т.д.) и где (верхнее, нижнее, левое и правое поле) размещать печатаемые элементы.

3. Программа обработки электронных таблиц отправляет файл печати на принтер.
4. Локальное сетевое ПО (предположим, что это редиректор Windows XP) распознает, что принтер находится в сети, и посылает запрос на печать серверу печати, чтобы напечатать этот файл. Редиректор получает информацию об имени и о сетевом адресе через сетевую службу Windows (именуемую Browse Service, которая обращается к серверу просмотра сети), чтобы выяснить, куда отправлять файл печати.
5. Со стороны сервера процесс-слушатель распознает и проверяет пользовательский запрос на печать. Мы будем предполагать его допустимым, так что процесс-слушатель создает временный поток выполняемых задач, чтобы обработать доставку пакетов входящего файла печати с клиента. Этот временный поток приказывает клиенту начать отправку файла печати.
6. Получив разрешение начать доставку файла, стек протоколов на клиенте разделяет файл на мелкие порции (называемые *пакетами),* которые доставляются временному потоку на сервере.
7. Временный поток на сервере наблюдает за доставкой файла и помещает его во временную область хранения, которая называется *файлом подкачки или спул-файлом (spool file),* где сервер печати хранит все ожидающие задания на печать. Сервер печати помещает задание в *очередь заданий на печать (print queue) в* порядке получения.
8. Когда задание на печать достигает начала очереди, сервер создает другой временный поток для доставки задания на принтер. Во многих случаях данные переносятся с сервера на принтер с помощью протокола, отличного от того, который в первую очередь использует клиент для доставки данных на сервер
9. На заключительном (и необязательном) шаге сервер печати создает еще один временный поток для отправки сообщения клиентскому компьютеру о том, что задание на печать завершено. Здесь для отправки сообщения обратно клиенту зачастую используется тот же протокол, что и для транспортировки файла с клиента на сервер.

На что здесь важно обратить внимание, так это на характер диалога, который происходит между клиентом и сервером. Клиент инициирует этот диалог, когда спрашивает разрешение на печать, а затем отсылает задание на печать серверу печати. Начиная с этого места сервер берет инициативу на себя, запоминая входящий файл печати в своем спул-файле и управляя очередью, а затем, когда приходит его очередь, распечатывает файл. Диалог завершается, когда сервер посылает уведомление о завершении задания клиенту.

Запросы на другие услуги (доступ к серверу баз данных, серверу электронной почты или даже файл-серверу) обрабатываются так же, как и для описанного выше взаимообмена. В подобных случаях диалог обычно завершается, когда сервер посылает таблицу данных, сообщение или файл в ответ на инициирующий запрос клиента. Последовательность "запрос-ответ" — это именно то, что заставляет работать современные сети.

Клиенты и ПО сетевого доступа

Если обратиться к истории, то самые неприятные проблемы с ПК были связаны с их работой в сети. До выпуска компанией Microsoft операционной системы Windows for Workgroups в 1993 году предшествующие версии — Windows 1.x, Windows 2.x и Windows 3.x, а также все версии DOS вплоть до Version 6.0 — не поддерживали встроенные сетевые возможности.

Таким образом, чтобы подключить ПК к сети, пользователь должен был не только заниматься установкой и конфигурированием сетевых адаптеров и программ-драйверов, которые заставляют их работать, *но* также покупать или иным способом получать ПО сетевых протоколов и сетевых служб от других поставщиков. Поскольку ни сами пользователи, ни Microsoft не могли обеспечить эти протоколы самостоятельно, такие продукты назывались *компонентами от сторонних поставщиков (third-party components).*

Достаточно сказать, что создание сети на основе ПК во времена, когда встроенные сетевые возможности отсутствовали, обычно означало добавление одного-двух сетевых продуктов от сторонних поставщиков к набору аппаратных и программных компонентов каждого компьютера. Обычно один из продуктов требовался для добавления стека протоколов, необходимого для сетевого взаимодействия, и один или несколько продуктов требовались для того, чтобы любые службы могли воспользоваться стеком протоколов для работы в пределах всей сети. Например, вам могло потребоваться приобрести стек протоколов наподобие TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Internet) для ПК от Chameleon Software, затем купить ПО электронной почты от QUALCOMM и связать их вместе с помощью интуиции и междометий.

Начиная с ОС Windows for Workgroups и затем многократно экспериментируя с Windows 95 и Windows NT, Microsoft значительно облегчила процесс создания сетей для простых смертных. Она добилась этого за счет того, что встроенные сетевые компоненты стали частью операционной системы. Хотя это усложнило жизнь сторонним поставщикам, которые неплохо жили за счет своих стеков протоколов и дополнительных сервисных продуктов, это, без сомнения, крайне упростило использование сетей. Это было особенно притягательно для пользователей, которые желали, чтобы сеть была чем-то таким, о чем можно сказать "установил и забыл", а не "установил и пожалел" или "помучился и переустановил"!

Сегодня Windows 98, Windows SE, Windows Me, Windows NT, Windows 2000, Windows XP и Windows 2003 включают все необходимые элементы для создания сети — от различных стеков протоколов до самых разнообразных клиентских и серверных возможностей. Если вы создаете свою сеть полностью на технологиях Microsoft или если большая часть ваших клиентов и серверов использует технологии Microsoft, работа с сетью полностью аналогична работе с другими частями операционных систем Windows. Другими словами, вы по-прежнему должны кое-что знать о том, что вы делаете (вот для чего вы читаете эту книгу, не так ли?), но вам нет нужды быть специалистом в ракетно-космической технике, чтобы устанавливать, конфигурировать и сопровождать необходимые протоколы и сервисные компоненты.

Однако в некоторых безвыходных ситуациях вам, возможно, придется повозиться с сетевыми компонентами от сторонних поставщиков, как во время оно. Например, ваша сеть может использовать сервер не от Microsoft, например NetWare или UNIX, чтобы обеспечить сетевые службы. Или, возможно, набор встроенных сетевых служб, поставляемых с Windows XP или Windows 2003, не содержит именно той, которая вам необходима, и вы должны добавить ее к набору самостоятельно.

Примером полезного компонента, который вы можете решить добавить сами, является сетевая файловая система *Network File System (NFS).* В сетях, которые базируются на ОС UNIX, NFS играет такую же роль в совместном использовании файлов, как встроенное разделение файлов в сетях Microsoft. Если вы желаете использовать эту возможность в Windows XP или Windows 2003, вы можете купить и установить дополнительный пакет под названием Microsoft Windows Services for UNIX. Сторонние поставщики, такие как Sun Microsystems (компания, где изобрели NFS) и Intergraph (поставщик самой быстродействующей реализации NFS для Windows), также предлагают NFS.

С 1993 года разработчики ПО прошли долгий путь, стремясь сделать интерфейс своих продуктов более похожим на Windows, а процесс их установки и конфигурирования более интуитивно понятным для администрирования. Сегодня вы, как правило, можете найти спра-

вочные файлы и мастер-программы, которые помогут вам при установке и конфигурировании компонентов сторонних разработчиков. Кроме того, многие функции сетей сторонних поставщиков используют сетевые возможности, присущие Windows, почти без изменений или с небольшими вариациями.

При выборе между встроенными сетевыми компонентами от Microsoft и альтернативами от сторонних поставщиков (которые мы подробно рассмотрим в главах 3 и 8) фактором, имеющим решающее значение, является тип функциональности, который требуется вашим клиентам. Некоторые функциональные возможности клиентского ПО, предлагаемые сторонними поставщиками, могут не работать в "родной" среде Microsoft. Если эти компоненты от сторонних производителей не работают с компонентами от Microsoft, вам, возможно, придется сравнить требования к этим функциональным возможностям продуктов независимых поставщиков со сложностью установки и конфигурирования сетевого ПО от независимых поставщиков.

Если требования к ПО сторонних поставщиков не подлежат обсуждению или их функциональные возможности имеют существенное значение, у вас нет другого выбора, как проглотить горькую пилюлю и смело посмотреть в лицо возможному кошмару конфигурирования. Например, доступ к определенным функциям драйверов в клиентском ПО NetWare, которые не поддерживаются Microsoft, могут заставить вас использовать ПО компании Novell — нравится вам это или нет. В противном случае вам придется втиснуться в рамки собственного клиентского ПО от Microsoft.

Встроенные функции и сетевые расширения

Иногда вам может потребоваться предоставить доступ клиентам к сетевым службам, которые не встроены в клиентское ПО Microsoft Windows. Предоставление пользователям доступа к этому типу функциональных возможностей всегда требует дополнительного ПО, подобного тому, которое необходимо для доступа к NFS. Хотя все последние версии Windows — Windows 95, Windows 98, Windows SE, Windows Me, Windows NT, Windows 2000, Windows XP и Windows 2003 — способны поддерживать NFS, эта поддержка не встроена в эти операционные системы. Поэтому, чтобы обеспечить пользователям доступ к NFS, требуется приобрести, установить и сконфигурировать дополнительное ПО на их компьютерах.

Добавление нового ПО к сетевым клиентам наподобие установки приложения в ОС Windows далеко не такое травмирующее (и более распространенное), как ситуация, описанная в предыдущем разделе, в которой вы должны были заменить клиентское ПО от Microsoft на клиентское ПО от Novell. Приложение должно быть совместимо с этой операционной системой, и вы должны корректно его установить и сконфигурировать. Однако ПО, которое использует только существующие протоколы и драйверы на машине, работающей по управлением Windows, расширяет встроенные возможности Windows, а не заменяет (или вытесняет) их. Поэтому добавление в Windows XP и Windows 2003 совместимых продуктов, таких как пакет электронной почты Eudora от QUALCOMM, программа передачи файлов WS_FT Pro от Ipswitch или Web-броузер Navigator от Netscape, — довольно легкое дело.

Тем не менее многие сетевые администраторы стараются не добавлять без необходимости протоколы и службы в Windows. Они поступают так из-за того, что каждый дополнительный протокол и служба потребляет системные ресурсы, такие как оперативная память и дисковое пространство. Будучи установленными, дополнительные протоколы и службы могут и не потребовать много оперативной памяти, если они никогда не используются или редко используются, но дисковое пространство службы всегда будут занимать!

Одним из наиболее основательных способов повышения производительности машины, работающей под управлением Windows 2003, является исключение ненужных протоколов и служб, а также *связывание* (*binding*), которое объединяет протоколы и службы. По умолчанию Windows 2003 связывает все протоколы и службы, даже если это связывание не является необходимым (или желаемым). Поэтому небольшая чистка после установки может повысить производительность так же, как и удаление ненужных программных соединений. Это справедливо для всех версий Windows, начиная с Windows for Workgroups 3.11. (Управление связыванием описывается в главе 18.)

Добавление клиентских приложений и служб от сторонних поставщиков на машину, работающую под Windows, не вызывает затруднений, поскольку большая часть подобного ПО в скрытом виде использует встроенные возможности Windows.

Управление сетевыми компонентами

Современные операционные системы Windows, под которыми мы понимаем Windows 95, Windows 98, Windows SE, Windows Me, Windows NT, Windows 2000, Windows XP и Windows 2003, включают поддержку для двух наборов сетевого клиентского ПО.

- ✓ *Clientfor Microsoft Networks* (Клиент для сетей Microsoft).
- ✓ *Client for NetWare Networks* (Клиент для сетей NetWare) (или *Client Service for NetWare* (Клиентская служба для NetWare)).

Эти два набора клиентского ПО показаны на рис. 2.1, на котором приведена вкладка General (Общие) объекта Local Area Connection Properties (Подключение по локальной сети: Свойства) системы Windows Server 2003. Эти два различных набора клиентского ПО обеспечивают доступ к двум различным наборам сетевых ресурсов.

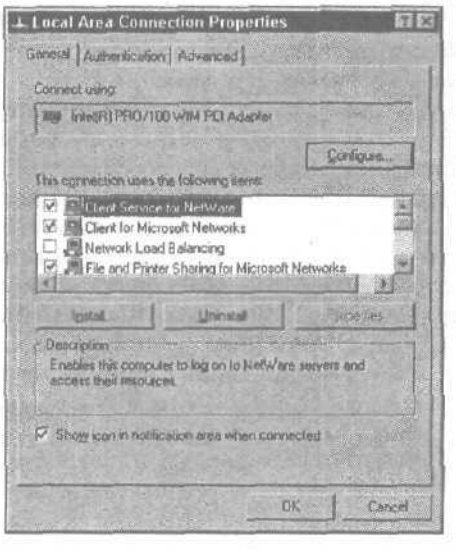
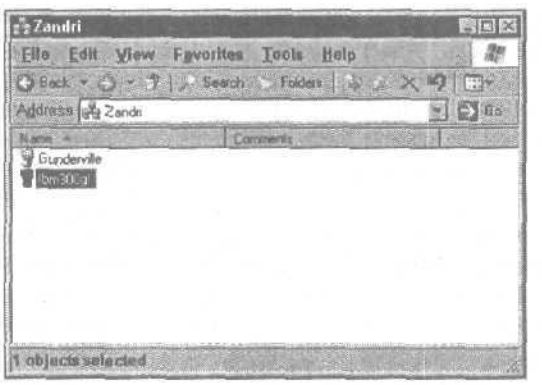


Рис. 2.1. Вкладка General объекта Local Area Connection системы Windows Serve 2003

Клиент для сетей Microsoft, **как** предполагает его название, включает необходимые компоненты для работы в качестве клиента в сети Microsoft. Клиент для сетей NetWare содержит аналогичные компоненты, требуемые для работы в качестве сетевого клиента NetWare. Дополнительные программные компоненты вступают в силу на сервере Windows Server 2003 и на клиентской машине под управлением Windows 95, Windows 98, Windows SE, Windows Me, Windows NT, Windows 2000 и Windows XP. Все эти компоненты мы рассмотрим в главе 8.

Чтобы ознакомиться с информацией о ресурсах, доступных в вашей сети, воспользуйтесь утилитой Windows 2003 под названием My Network Places (Мое сетевое окружение). По умолчанию эта пиктограмма отображает список всех сетевых совместно используемых ресурсов и компьютеров, на которых они размещены. Однако вы можете настроить ее так, чтобы она показывала все виды отображений. Например, на рис. 2.2 вы видите полный перечень всех компьютеров в одном из доменов в виде списка машин.



Рис, 2.2. Утилита My Network Places показывает, какие компьютеры есть в вашем ближайшем сетевом окружении

Сеть Microsoft: кто под маской

Помимо основных сетевых клиентских компонентов, используемых Windows Server 2003 для взаимодействия с сетями на базе ОС компаний Microsoft и NetWare, для функционирования сети важное значение имеет целый ряд других компонентов.

- ✓ **Многопротокольный маршрутизатор (MultiProtocol Router — MPR).** Распределяет запросы на сетевые услуги специальному *поставщику сетевых услуг (network provider),* который представляет определенный тип сетевой клиентской среды. (Он направляет запросы на сетевые услуги Microsoft поставщику сетевых услуг Microsoft, а запросы на сетевые услуги NetWare — поставщику сетевых услуг NetWare.) MPR позволяет системе Windows поддерживать одновременно несколько соединений. MPR также определяет общий интерфейс, так что приложения могут осуществлять доступ к общим функциональным возможностям всех сетей посредством единого набора вызовов интерфейса.
- ✓ **Поставщик сетевых услуг Microsoft (Microsoft Network Provider).** Определяет открытый интерфейс, который позволяет сторонним поставщикам интегрировать в систему поддержку для своих сетей. Поставщик сетевых услуг Microsoft также предоставляет доступ (и управление) к сетевым ресурсам и компонентам посредством общих утилит, таких как My Network Places и Network Connections (Сетевые

соединения). Поставщик сетевых услуг Microsoft обеспечивает единый набор хорошо структурированных функций для просмотра серверов, установления и разрыва соединений с серверами и взаимодействия с другими сетевыми ресурсами.

- ✓ **Устанавливаемый менеджер файловой системы (Installable File System Manager — IFSMGR).** Этот набор функций доступа к файловой системе интегрирует несколько файловых систем посредством единого интерфейса. IFSMGR позволяет рассматривать запросы на доступ к удаленной файловой системе точно так же, как запросы на доступ к локальной файловой системе с точки зрения их структуры и функций. (Они отличаются только способом адресации запрашиваемых объектов.)
- ✓ **Редиректор клиента для сетей Microsoft (Client for Networks Redirector).** Этот программный компонент проверяет все запросы приложений на ресурсы. Она передает любые запросы на удаленные ресурсы сетевому интерфейсу и пропускает запросы на локальные ресурсы к локальной операционной системе.
- ✓ **Интерфейс NetBIOS.** Этот протокольный интерфейс определяет высокоуровневый протокол запросов/ответов, который доставляет запросы к удаленным ресурсам (и их ответы). В частности, интерфейс NetBIOS использует специальный протокол обмена сообщениями под названием *Server Message Block (SMB) (Блок серверных сообщений)* для транспортировки запросов от клиентов к серверам и ответов на эти запросы от серверов к отправившим их клиентам.
- ✓ **Сетевые протоколы, разработанные для поддержки спецификации интерфейса сетевых драйверов Microsoft (Network Driver Interface Specification — NDIS) версии 3.1 и выше.** Эти компоненты относятся к встроенным сетевым протоколам для ОС Windows, дальнейшее обсуждение которых будет продолжено в главе 3.
- ✓ **Общий интерфейс NDIS.** Это соглашение по программированию определяет стандартный программный интерфейс с сетевыми адаптерами в ОС Windows. Оно позволяет разработчикам драйверов взаимодействовать с сетевыми адаптерами с использованием широко известного и хорошо документированного набора программных вызовов для пересылки данных из компьютера в адаптер для исходящих сообщений и из адаптера в компьютер — для входящих сообщений.
- ✓ **Специальный драйвер адаптера NDIS.** Этот драйвер устройства преобразует формат общего сетевого интерфейса в специфический формат для некоторого сетевого адаптера (или адаптеров), установленного на компьютере, работающем под Windows. (Обратите внимание, что Windows NT, Windows 2000, Windows XP и Windows 2003 поддерживают несколько адаптеров на одной машине, но ни Windows 95, ни Windows 98 не предоставляют такой возможности.)

На рис. 2.3 показаны рассмотренный выше набор сетевых компонентов Microsoft и способы взаимодействия различных компонентов с приложениями, которые осуществляют запросы, а также с сетью, которая переносит эти запросы на сервер и доставляет соответствующие ответы на эти запросы. Обратите, пожалуйста, внимание на то, что хотя все операционные системы Windows имеют аналогичную конструкцию и используют аналогичные компоненты, все же между отдельными ОС существуют различия в деталях.

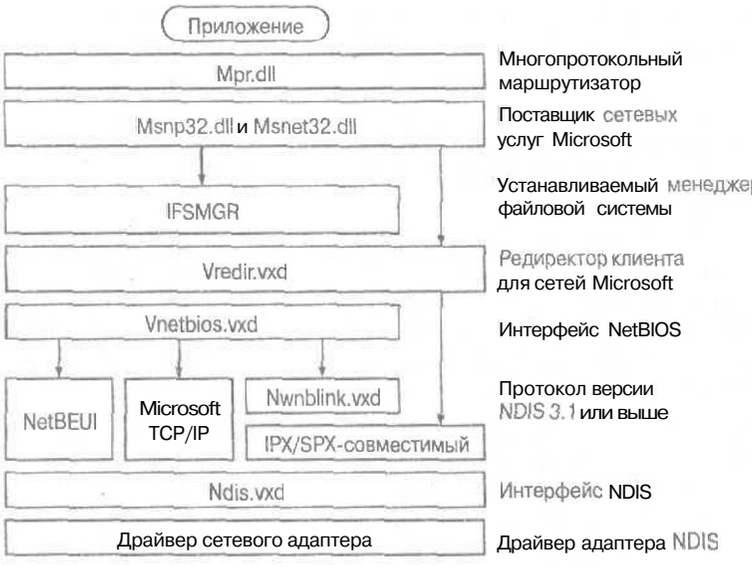


Рис. *2.3. Структура компонентов ПО Clientfor Microsoft Networks*

Знакомство с сетью Novell

Хотя компонентная структура Client for NetWare Networks и аналогична структуре ПО Client for Microsoft Networks (о котором речь шла в предыдущем разделе), различия между ними кроются в специфических ориентированных на NetWare компонентах, которые заменяют своих двойников от Microsoft. Вместо компонентов от Microsoft на многих этапах сетевого пути от приложения до драйвера NDIS используются компоненты, специфические для NetWare. Приведем результирующий набор компонентов.

- **Многопротокольный маршрутизатор (MPR).** Этот программный компонент является общим для всех сетевых клиентов операционных систем Windows. Так же как и в случае сети Microsoft и сети Microsoft для Windows, MPR переправляет запросы на услуги соответствующему поставщику сетевых услуг.
- **Поставщик сетевых услуг, совместимый с NetWare.** Этот программный компонент обеспечивает доступ и управление доступными в NetWare сетевыми ресурсами и компонентами с помощью общих утилит, таких как My Network Places и Network Connections. Подобно его двойнику от Microsoft, совместимый с NetWare поставщик сетевых услуг обеспечивает единый набор хорошо структурированных функций для просмотра серверов, установления и разрыва соединений с серверами и взаимодействия с другими сетевыми ресурсами.
- **Устанавливаемый менеджер файловой системы (IFSMGR).** Этот набор функций доступа к файловой системе интегрирует несколько файловых систем посредством единого интерфейса для согласованного локального и удаленного доступа к файлам и ресурсам печати NetWare при работе ПО Client for NetWare Networks.
- **Редиректор клиента для сетей NetWare.** Этот программный компонент передает любые запросы на удаленные ресурсы сетевому интерфейсу NetWare и пропускает запросы на локальные ресурсы к локальной операционной системе.

- **Один из нескольких сетевых протоколов.** Клиент для сетей NetWare может использовать для доступа к сети либо протокол IPX/SPX (Internet Packet eXchange/Sequenced Packet eXchange — межсетевой обмен пакетами/последовательный обмен пакетами), либо TCP/IP.
- **Общий интерфейс NDIS.** Этот драйвер устройства определяет стандартный интерфейс с сетевыми адаптерами в ОС Windows. Один и тот же интерфейс работает с клиентами Microsoft и NetWare.
- **Специальный драйвер адаптера NDIS.** Этот драйвер устройства преобразует формат общего сетевого интерфейса в специфический формат для некоторого сетевого адаптера (или адаптеров), установленного на компьютере, работающем под Windows. (Обратите внимание, что Windows NT, Windows 2000, Windows XP и Windows 2003 поддерживают несколько адаптеров на одной машине, но ни Windows 95, ни Windows 98 не предоставляют такой возможности.)

Седует отметить, что в этом наборе отсутствует отдельный интерфейс NetBIOS. Этот пробел означает, что NetWare не использует имена NetBIOS для навигации по своей сети. Клиент для сетей NetWare ничего не утрачивает из своих возможностей в отношении NetBIOS, даже несмотря на то, что отдельный интерфейс NetBIOS отсутствует, приложения по-прежнему нуждаются и получают поддержку NetBIOS. Заметьте также, что маршрутизатор MPR, устанавливаемая файловая система, протоколы (за исключением выбираемого диапазона) и компоненты NDIS остаются более-менее одинаковыми как для клиентов Microsoft, так и для клиентов NetWare.

Глядя на эту компонентную структуру ПО, вы можете спросить, можно ли сочетать и отождествлять программные компоненты от Novell и Microsoft. К сожалению, при установке программных компонентов сетевого клиента на машине, работающей под управлением Windows, вы все время должны идти либо одним путем (Microsoft), либо другим (Novell). Попытка использовать оба ни к чему хорошему не приведут!

Вы можете без труда запустить оба клиента — и от Microsoft, и от Novell, — но вы не можете использовать компоненты Novell и Microsoft на любой машине под управлением Windows. Поэтому вы можете использовать ПО от Microsoft для доступа к серверам Windows Server 2003 и NetWare или ПО от Novell для доступа к серверам Windows Server 2003 и NetWare. Но вы не можете использовать ПО от Microsoft для доступа к серверам Windows Server 2003 и ПО NetWare для доступа к серверам NetWare на одной и той же машине.

Управление доступом к ресурсам

Часть каждого запроса на сетевой ресурс, который делает клиент, содержит собственную идентификацию клиента. Другая часть именует ресурсы, которые клиент запрашивает из сети. Обычно для доступа к ресурсам в одноранговой сети клиент использует пароль, который Microsoft называет *контролем доступа на уровне разделяемого ресурса* (*share-level access control*), поскольку каждый пароль применяется к одному разделяемому ресурсу,

В сети Microsoft "клиент/сервер" уровень прав пользователя управляет возможностями этого пользователя по доступу к ресурсам. На языке Microsoft *доступ на уровне пользователя (user-level access)* означает, что когда пользователь идентифицирует себя в запросе на обслуживание, учетное имя пользователя определяет, какие запросы сервер может "уважить", а какие он должен отклонить.

Сервер проверяет, на какие ресурсы пользователь обладает правами доступа, а также допустима ли операция, запрашиваемая пользователем. Например, Боб может **иметь** разрешение на чтение определенного файла, но может не иметь прав на запись в файл или его удаление. Если он запрашивает операцию чтения, запрос пропускается, если же он запрашивает операцию записи или удаления, запрос отклоняется.

Обработка запросов в сети "клиент/сервер" требует большего объема работы, чем может показаться на первый взгляд; это, в частности, связано с *проверками безопасности (security check),* которые контролируют доступ и ограничения в сети. Установление прав требует понимания того, какие **имена** приписывать ресурсам, доменам, в которых эти ресурсы размещаются, и пользователям, которые формулируют подобные запросы. Большая часть материала, который содержится в главах 8, 11-14 и в особенности в главах 15,16 и 18, касается этих терминов и понятий и объясняет их глубинный смысл.

Примеры сетевых служб Windows

В предыдущих разделах мы рассказали о механизме запросов-ответов, который управляет всеми запросами на сетевые услуги, а также о способах формирования ответов. В этом разделе мы объясним, что вы можете делать в рамках этой структуры. Ниже приведен перечень общих служб, которые вы, скорее всего, обнаружите в сети на основе сервера Windows Server 2003.

- ✓ **Обработчик извещений (Alerter).** Обеспечивает возможность отправки аварийных сигналов и извещений определенным получателям при наступлении событий, фиксируемых программой Event Viewer (Просмотр событий), или превышении пороговых значений, фиксируемых программой System Monitor (Системный монитор).
- ✓ **Служба просмотра сети (Computer Browser).** Управляет списком имен компьютеров и ресурсов для определенной сети, так что пользователи могут просмотреть список и узнать, что там находится (и доступно), с помощью утилиты Network Neighborhood (Сетевое окружение) или других утилит.
- ✓ **Служба доставки сообщений (Messenger).** Служит для Windows Server 2003 средством доставки экранных сообщений определенным получателям в ответ на явные команды или аварийные сигналы и извещения.
- ✓ **Служба входа в сеть** (Net **Logon).** Управляет попытками пользователя войти в сеть и переносит информацию ото всех контроллеров доменов в один домен Windows Server 2003.
- ✓ **Служба сетевого обмена DDE (Network DDE).** Позволяет динамически распространять обновления файлов и документов, происходящие в пределах сети. *Динамический обмен данными (Dynamic Data Exchange — DDE)* — это динамическая технология обновления, используемая для копирования изменений одного файла или документа в другой, когда встроенные объекты в одном документе должны отражать изменения этого объекта в другом.
- ✓ **Поставщик поддержки безопасности** NT LM (NT **LM Security Support Provider).** Обеспечивает модель безопасности Windows Server 2003, совместимую с LAN Manager (LM). Эта служба работает с шифрованием и доставкой запросов на вход в сеть, которые не могут использовать более современные модели безопасности Windows.

- **Поддержка технологии Plug and Play.** Обеспечивает совместимость машины, работающей под управлением Windows 2003, со стандартом Plug and Play. (Plug and Play — "включай и работай". Стандарт фирм Microsoft, Intel и др., преследующий цель упрощения подключения компьютера; берет на себя распознавание и настройку периферийного устройства без последующей установки параметров пользователем. — *Прим. ред.).*
- **Спулер принтера (Print Spooler).** Манипулирует хранилищем файлов для ожидающих в очереди заданий на печать. Это служба, которая управляет планированием и сохранностью ожидающих заданий на печать, пока не наступит их очередь печати.
- **Служба маршрутизации и удаленного доступа (Routing and Remote Access Service — RRAS).** Охватывает целый ряд услуг RRAS. Обеспечивает услуги коммутируемой связи для более чем 256 одновременных соединений на один сервер Windows Server 2003, а также предоставляет набор услуг маршрутизации.
- **Сервер** (Server). Функционирует как основной процесс-слушатель запросов на обслуживание на сервере Windows Server 2003. (Фактически остановка службы Server — неплохой способ временного запрещения сетевого доступа к серверу.) Хотя название этой службы может говорить об ином, эта служба должна быть размещена как на клиентской машине Windows, так и на машине, которая работает под управлением Windows Server 2003.
- **Служба телефонии (Telephony** Service). Дает возможность Windows 2003 использовать встроенный интерфейс Windows TAPI (Telephony Application Programming Interface — интерфейс прикладного программирования для телефонии) для доступа к модемам, телефонам, ISDN-сетям (Integrated Services Digital Network — цифровая сеть с комплексными услугами) и линиям xDSL (цифровые абонентские линии) посредством стандартного наборного устройства и интерфейса телефонной книги. Таким образом, эта служба также является ключевым компонентом службы RRAS.
- **Рабочая станция (Workstation).** Позволяет машине, на которой функционирует Windows 2003, выдавать запросы на обслуживание. Это служба поддержки работы клиента,

Чтобы просмотреть исчерпывающий перечень служб, доступных в Windows 2003, обратитесь к утилите Services (Службы), которая появляется в разделе (Administrative Tools) (Средства администрирования) меню Start (Пуск) или Control Panel (Панель управления).

Хотя этот длинный список не включает все службы Windows Server 2003, в нем представлены наиболее часто используемые службы, которые вы, вероятно, можете найти на большинстве компьютеров. В последующих главах вы узнаете, что могут эти службы, а также как их установить, конфигурировать и сопровождать.

Глава 3

Вопросы протокола

В этой главе...

- Роли, которые берут на себя протоколы
- Управление сетевым доступом — задача номер один!
- Перемещение данных из приложения в сеть и обратно
- Собираем компанию: протоколы не ходят по одному
- Представление о протоколах IPX/SPX и NWLink
- Знакомство с TCP/IP: протокол для Internet
- Другие протоколы

В этой главе мы рассмотрим сетевое взаимодействие и сообщения, которые перемещаются по сети. Мы более подробно расскажем о том, что посылает отправитель и что принимает получатель, а по ходу дела вы получите сведения о наборах правил, называемых *протоколами,* которые определяют способы обмена информацией между компьютерами в сети.

По существу, сетевое взаимодействие основано на общем для всех его участников наборе правил обмена информацией, которые определяют, как выглядят данные на самом элементарном уровне. В частности, речь идет о том, как представить данные в цифровом виде (или что такое "единица" и что такое "нуль"?). Эти правила также обусловливают формат сетевых адресов и смысл, скрытый за этими адресами, которые указывают, что в сети означают понятия "здесь" и "там", идентифицируют тип и содержимое сообщений и дают массу другой полезной и крайне необходимой информации.

Как общаются компьютеры

Способы взаимодействия компьютеров и стили общения людей имеют много общего. Возьмем, к примеру, телефонный звонок.

- ✓ Телефонные звонки начинаются с весьма шаблонного установления контакта между соответствующими собеседниками на обоих концах соединения. ("Скажите, это квартира Флогистон? Могу ли я поговорить с Филом?") Компьютеры используют аналогичную линию поведения для сетевого взаимодействия, так как отправитель зачастую начинает с вопроса получателю о том, возможен ли разговор, и только после получения разрешения происходит некий фактический обмен данными.
- ✓ Смена очередности в телефонном разговоре требует умения внимательно слушать и соблюдать паузы в разговоре с противной стороной, так что каждая сторона может говорить, когда появляется возможность. У компьютеров отсутствует интуиция, так что они обмениваются явными сигналами, когда одна из сторон желает прекратить "слушать" и начать "говорить". В действительности некоторые методы коммуникации позволяют обеим сторонам говорить и слушать одновременно!

- ✓ Телефонный разговор может быть завершен по взаимному согласию или после того, как одна из сторон подаст другой недвусмысленный знак, свидетельствующий о ее желании закончить разговор. (Известным примером является фраза "Ну что ж, не смею вас больше задерживать".) Компьютеры также обмениваются сигналами, чтобы показать, что сетевой "разговор" близится к концу, а затем завершают его, разрывая соединение друг с другом.
- ✓ Люди обладают умением перенимать опыт, которое помогает им распознавать ситуации непредвиденного окончания разговора, такие как отказ батарейки радиотелефона, выход за пределы зоны, охваченной сотовой связью, или полный отказ соединения. У них также хватает сообразительности повторить попытку или отказаться от дальнейших попыток связаться с абонентом, в зависимости от того, достигли ли они цели своего контакта или нет. Компьютеры более просты; они ожидают, пока связь не возобновится либо не истечет фиксированный интервал времени (называемый *тайм-аутом),* прежде чем распознают, что соединение не действует и разговор закончен. Затем это доходит до приложения, инициировавшего связь, которое решает, возобновить ли дальнейшие попытки или отказаться от них.

Понимание различий между общением людей и взаимодействием компьютеров поможет вам лучше понять природу компьютерных сетей. Представляется, что самое большое отличие состоит в том, что люди несравненно лучше действуют, пользуясь своей интуицией и опытом, чем компьютеры.

Ключ - в интерпретации...

То, что мы говорим (или слышим), общаясь по телефону, всегда определенным образом интерпретируется и зачастую истолковывается неверно. Тот смысл, который вы вложили в свои слова, может быть неправильно понят вашим собеседником. В основе человеческого общения лежат общедоступные правила и смысл, а также общая точка зрения. Процесс взаимодействия компьютеров также основан на этих элементах; однако поскольку компьютеры не наделены интуицией и не способны рассуждать, эти элементы должны быть полностью расшифрованы. Компьютеры могут выполнять только то, на что они запрограммированы.

Для обмена данными между компьютерами каждый элемент должен подаваться явно. Компьютеры не могут улавливать подтекст и скрытый смысл. Чтобы осуществлять взаимодействие, компьютеры должны начать с детального согласования следующих вопросов (с компьютерной "точки зрения").

- ✓ Каков мой адрес? Как я могу узнать мой адрес? Как я могу узнать адреса других компьютеров?
- ✓ Как я могу подать сигнал другому компьютеру, чтобы показать, что я готов отправить (или получить) сообщение, что я занят или не могу ждать, если он занят?

Если вы представите себе телефонную систему, эти вопросы будут аналогичными для звонка человека по телефону и для звонка компьютера по модему. Фактически эти вопросы можно переформулировать следующим образом.

- ✓ Каков мой телефонный номер? Как я могу узнать мой телефонный номер? Как я могу узнать номера телефонов других лиц или организации, с которыми я желаю связаться?
- ✓ Как я могу заказать разговор по телефону? Как я могу распознать сигнал "занято"? Как я могу заставить телефон продолжать набор, если номер, с которым я желаю связаться, занят? (Заметьте также, что телефонная система обрабатывает сигналы "занято" и "вызов", так что и компьютер, и человек могут сказать, когда звонок прошел, а когда необходимый абонент занят.)

Договоримся о правилах

Создание полного и согласованного набора правил для взаимодействия компьютеров — трудоемкое, кропотливое дело, которое вполне может свести большинство обычных людей с ума. Назаре развития компьютерной индустрии отдельные компании набирали множество программистов для написания программ компьютерных коммуникаций, чтобы решить специфические, отдельные проблемы.

Но со временем программисты поняли, что этот подход создает слишком много уникальных способов взаимодействия компьютеров, которые работают только в пределах небольших, технически изолированных коллективов. После того как увеличилась потребность в коммуникации, существенная несовместимость; препятствовала обмену данными между подобными коллективами до тех пор, пока один из коллективов добровольно не отказывался от своего способа взаимодействия и не принимал на вооружение другой способ.

Правительство США сыграло ключевую роль в наведении порядка в этом сетевом хаосе. Когда правительство пыталось получить компьютеры от компании А, чтобы работать с компьютерами компании Z, оно вскоре поняло, что столкнулось с чудовищной проблемой совместимости. Вскоре общими усилиями было выработано мнение, что для облегчения работы сетей необходим общий набор правил. Также пионеры в области сетевых технологий быстро осознали, что создание сетей было трудным, если не совершенно безнадежным делом из-за того, что никто не следовал одним и тем же правилам.

Если бы у этой сказки был действительно сказочный конец, он бы звучал так: "Сегодня существует только один набор правил создания сетей, которым все благоразумно и с готовностью пользуются". Увы, это не соответствует действительности. Хаоса в создании сетей стало значительно меньше, но многие наборы взаимно несовместимых сетевых протоколов по-прежнему используются, поскольку производители программного и аппаратного обеспечения стремятся быть "на переднем крае борьбы по выживанию денег", изобретая новые правила по мере того, как отважно вторгаются в области, где раньше о сетях и не слышали.

Чтобы компьютеры могли взаимодействовать в пределах сети, необходимо ответить на эти основополагающие вопросы, а ведь они составляют лишь малую часть большого и сложного множества деталей, которые требуется проработать, систематизировать и реализовать. Ответы на все эти вопросы составляют основу набора правил для взаимодействия компьютеров; фактически эти правила представляют собой "правила дорожного движения" — или протоколы — для создания сетей.

Следуем протоколу

Наборы правил, о которых мы говорили в предыдущем разделе, обычно называются *сетевыми протоколами (networking protocol),* но иногда их также называют *сетевыми стандартами, стандартными сетевыми протоколами* и т.п. Идея заключается в следующем: эти правила совместно используются некоторой группой, которая стремится общаться внутри себя и определяет общий метод для компьютеров, чтобы общаться друг с другом. Каждый конкретный протокол определяет язык, структуру и набор правил для поддержки подобного взаимодействия.

В определение набора сетевых протоколов вкладывается большой труд, и еще большего труда требует создание ПО для его реализации. Это масштабный проект, и объем работы, необходимый для того, чтобы справиться с ним, объясняет, почему пользователи, разработчики и производители ПО считают удобным придерживаться протоколов, которые наилучшим образом удовлетворяют их нужды.

В дипломатии протокол устанавливает строгий набор процедур и правил этикета, которым следуют представители суверенных держав, чтобы предотвратить тотальную войну. Например, протокол помогает объяснить, почему в случае абсолютного совпадения мнений ди-

пломаты говорят об "открытой и искренней дискуссии", а о сложных разногласиях, как о "конструктивном диалоге". Если оставить в стороне политическое лицемерие, слово *протокол* довольно хорошо передает сущность правил для сетевого взаимодействия.

Наборы протоколов

Хотя эта книга посвящена преимущественно Windows Server 2003 и протоколам, разработанным компанией Microsoft, протоколы, включенные в Windows 2003, представляют только часть многочисленной совокупности широко распространенных и хорошо структурированных сетевых протоколов. Microsoft сделала хорошее дело, разрешив одновременное функционирование многих типов протоколов в рамках Windows 2003, включая стандарт для Internet — TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Internet) и стандарт от компании Novell — IPX/SPX (Internet Packet eXchange/Sequenced Packet exchange — межсетевой обмен пакетами/последовательный обмен пакетами).

При изучении любой сетевой реализации вы, скорее всего, обнаружите, что протоколы редко, если такое вообще случается, появляются по одиночке. Большинство сетевых протоколов состоят из совокупности специальных форматов сообщений и правил взаимодействия, обладающих своими собственными именами и функциями, а не из единой, неделимой совокупности форматов и правил. По этой причине протоколы можно также назвать *свитами протоколов*. (Здесь игра слов: по-английски *свита* и *набор (комплект)* пишутся как *suite*. Так что на самом деле речь, конечно, идет о *наборах протоколов, — Прим. ред.*)

Становление стандартов

Интересно отметить один факт, касающийся сетевых правил: как поставщики сетевых решений, так и группы-разработчики стандартов называют свои протоколы ***стандартами.*** Некоторые поставщики красноречиво рассуждают о различии между стандартами де-факто и де-юре. Стандарт ***де-факто*** означает: "Это не официальный стандарт, но уйма людей использует его, поэтому мы, при желании, можем называть его стандартом". Стандарт ***де-юре*** означает: "Это стандарт, потому что ABC (организация, устанавливающая стандарты) объявила его таковым и в подтверждение этого опубликовала кипу книг!"

В пылу жарких дискуссий о том, что является, а что не является стандартом, остается незамеченным главный вопрос. Борцы за чистоту стандартов, включая ученых, исследователей и "знатоков", категорически заявляют, что только организации-законодатели в области стандартов могут быть объективными и беспристрастными. Только эти организации могут отбирать лучшее из того, что могут предложить современные технологии, и перенести это лучшее в стандарты и установить, таким образом, наилучшие возможные стандарты.

Другим источником напряженности выступает отчаянная гонка производителей за сохранение своего места на рынке, а также за пользовательскими требованиями более совершенной, быстрой и дешевой технологии. Поставщики борются за то, чтобы получить готовый продукт и выпустить его на рынок. "Конечно, мы должны контролировать свою технологию, — говорят они. — Как иначе мы можем продержаться?"

Объективность, добросовестность и передовой характер большей части стандартов протоколов могут и не подвергаться обсуждению, но установление стандартов требует формирования рабочих групп, которые должны согласовать их содержание. Это требует времени. (Ничто не утрачивает новизну так быстро, как передовая технология.)

Неважно, являются ли сетевые протоколы стандартами или нет, и к какой категории — де-факто или де-юре — их отнести. Рынок — вот центр активности. Поставщики должны участвовать во всех дискуссиях, поддерживая все стороны, поскольку в гонке они должны ставить на всех технологических "лошадей". Некоторые дальновидные поставщики, включая Microsoft, публикуют свои стандарты и предоставляют в распоряжение потребителей и отраслевых экспертов достаточный объем документации, чтобы создавать работоспособные сети и в то же время сохранять высокий темп разработки.

Некоторые организации по стандартизации были достаточно благоразумны, чтобы понять, что жизнеспособны только широко используемые стандарты. Эти организации позволили поставщикам аппаратного и программного обеспечения рассматривать реальные проблемы, касающиеся выведения продуктов на рынок. Победителями в обоих лагерях являются наиболее распространенные протоколы. Microsoft выбрала для Windows Server 2003 (и других версий Windows) ведущий стандартный протокол TCP/IP и широко используемый протокол от стороннего поставщика IPX/SPX/NetBIOS (или NWLink) (Протоколы IPX/SPX появились вместе с системой NetWare компании Novell.)

Протоколы охватывают все аспекты сети

Если сформулировать одну ключевую концепцию, которая объясняет необходимость стандартов, то сущность ее, безусловно, в том, что протоколы управляют движением информации между оборудованием, подключенным к сетевому интерфейсу, и приложениями, которые осуществляют доступ к сети. Причина, по которой один компьютер не может общаться с другим компьютером без совместного использования общего набора протоколов, состоит в том, что как отправитель, так и получатель должны быть способны понимать операции, форматы данных и механизмы доставки своего партнера. Без такой общей точки зрения сеть не может работать.

Протоколы заполняют брешь между сетевым оборудованием и его ПО; они используются программами, которые дают возможность вашему компьютеру осуществить доступ к сети. Эти протоколы переправляют данные от приложений на всем пути вплоть до оборудования, где для общения с сетью протокол говорит: "Отправь это сообщение". Когда оборудование показывает, что пришло входящее сообщение, протокол идет по другому пути и говорит оборудованию: "Дай мне сообщение".

Большинство протоколов не заботит, с каким типом сети они переговариваются. Как правило, протоколы не имеют представления и об используемой сетевой технологии, которой может быть технология Ethernet, сеть Token Ring или нечто экзотическое. Эта индифферентность возможна благодаря тому, что часть ПО, которая обеспечивает доступ к аппаратуре, размещается в *драйверах устройств* для сетевого интерфейса. Сами по себе протоколы происходят от других источников (в Windows 2003 они размещаются в программных компонентах, установленных как часть операционной системы, до тех пор, пока на машину не устанавливаются компоненты сторонних поставщиков, которые замещают встроенные компоненты.) Поэтому, когда протокол обращается к сетевому интерфейсу, чтобы отправить или получить данные из сети, он в действительности связывается с ним через драйвер устройства. Определенный драйвер устройства в точности указывает протоколу, как обращаться к сетевому интерфейсу (или интерфейсам), установленному на вашей машине.

Как мы объяснили в главе 2, некоторые приложения включают встроенные сетевые возможности, которые используют специальные программные интерфейсы. Такие осведомленные о состоянии сети приложения становятся все более обычным делом по мере повсеместного распространения сетей. Большая часть приложений, разрабатываемых Microsoft, обладает некоторым сетевым интеллектом, но мощь этого интеллекта изменяется в зависимости от назначения и возможностей каждого приложения. Другие приложения могут использовать стандартный API-интерфейс (Application Programming Interface — интерфейс прикладного программирования) и так или иначе получать доступ к сети, будучи в полном неведении о ее существовании, Именно здесь вступают в игру редиректор и другие ключевые элементы системы. Способно ли приложение работать с сетью самостоятельно или использует внешние сетевые возможности, поскольку оно получает доступ к сети, то использует ПО протоколов (и драйверов устройств) для принятия входящих и отсылки исходящих сообщений.

Набор протоколов служит ключом, открывающим доступ к сети как приложениям, так и операционной системе. Как мы объяснили в главе *2,* Windows 2003 включает все компонен-

ты, необходимые для поддержки приложений, осведомленных о состоянии сети, и приложений, не имеющих о ней представления, что, несомненно, делает ОС Windows Server 2003 саму по себе достаточно "смышленой" в сетевых проблемах. И хотя приложения (и ОС) могут осуществлять запросы на сетевые услуги, всю "грязную работу" по отправке пакетов сообщений в пределах сети и последующей распаковке входящих сообщений для представления их в удобочитаемом (прежде всего, для приложений) виде берут на себя протоколы.

Другие ОС, такие как Windows 95, Windows 98, Windows SE, Windows Me, Windows NT, Windows 2000 и Windows XP, также обладают встроенным сетевым ПО, которое управляет сетевым интерфейсом, а также теми протоколами и службами, которые используют его. Однако система DOS и более старые версии Windows (Windows 3.*x*) используют клиентское сетевое ПО, поставляемое Microsoft с Windows Server 2003 (или другие альтернативы от сторонних поставщиков).

Сходство между протоколами и почтовой службой

Большая часть взаимодействий, которые происходят между приложением и аппаратными средствами, состоит в том, чтобы, по мере того, как сообщения удаляются от приложений и приближаются к оборудованию, взять сообщения, разобрать их на части и упаковать в конверты. В другом направлении движения — от оборудования к приложению — протоколы распаковывают конверты и повторно собирают отдельные части для восстановления полных сообщений. Мы всегда рассчитываем на то, что результирующее сообщение осмысленно, но не следует забывать GIGO, этот непреложный закон вычислительной техники — "если мусор на входе, то мусор и на выходе" (Garbage In Garbage Out).

Здесь может быть уместна аналогия с почтой. Почтовое отделение обрабатывает все почтовые отправления с указанным адресом, доставка которых оплачена в соответствии с принятыми тарифами и размеры которых являются допустимыми для письма или посылки. Как доставляется письмо? Это делается следующим образом.

1. Вы надписываете на конверте адрес, наклеиваете марку и бросаете его в почтовый ящик.
2. Почтовый перевозчик почты забирает письмо.
3. Почтовый перевозчик доставляет письмо в местное почтовое отделение.
4. Сортировщик почты проверяет почтовый код и распределяет письмо.
5. Письмо отправляется в почтовое отделение, которое обслуживает район, указанный в почтовом коде.
6. Сортировщик почты проверяет адрес дома (улица и номер дома) и направляет письмо соответствующему почтовому перевозчику.
7. Почтовый перевозчик доставляет письмо по адресу его получателя.

По меньшей мере это *предполагаемый* способ работы почты. Основными требованиями успешной доставки почты являются своевременный забор почты, короткое время пересылки и верная доставка. Время пересылки и доставка зависят от таких факторов, как верная идентификация адреса получателя и правильный выбор маршрута доставки, а также возможные задержки в пересылке между отправителем и получателем.

Сходство между сетевыми протоколами и почтовой службой лежит в способности распознавать адреса, направлять сообщения от отправителей к получателям и обеспечивать доставку. Основное различие состоит в том, что почтовая служба, в отличие от сетевых протоко-

лов, не заботится о содержимом отправляемых нами конвертов до тех пор, пока они соответствуют ограничениям по размерам, весу и материалу. В чем сетевые протоколы совершенно не похожи на почтальонов, так это в том, что они проявляют большую заботу о содержимом отправляемых конвертов. Одна из основных задач сетевого протокола состоит в разбивке содержимого конвертов и помещении его в конверты меньших размеров для доставки.

Предположим, например, что вам необходимо скопировать файл размером 10 Мбайт с вашего компьютера на другую машину вашей сети. Файл состоит из электронных таблиц с некоторыми графиками и рисунками, которые представляют прогноз сбыта на следующий квартал, поэтому вы хотели бы, чтобы он пришел быстро и корректно.

Чтобы воспользоваться почтой (или тем, что сетевые администраторы называют "улиточной почтой"), вы должны скопировать файл на флоппи-диск и отправить по почте его получателю. Однако для большинства пользователей компьютеров это недостаточно быстро. По сети эта операция займет около 30 секунд (в то время как при использовании обычной почты на это может уйти несколько дней). Когда ваш файл перемещается с вашей рабочей станции на другую машину, он распадается на множество мелких пакетов, а затем, по получении, восстанавливается в своем первоначальном виде — в файле объемом 10 Мбайт.

Ограничение объема, т.е. наибольшая порция данных, которая может перемещаться по сети в одном сообщении, лишь одна из причин того, что сетевые сообщения разбиваются и помещаются в отдельные конверты. Другая причина — обработка адресов. В примере с почтой почтовое отделение интересует почтовый код получателя, в то время как доставляющего почту перевозчика интересует только адрес дома. Аналогично, один протокол может заботиться только об имени компьютера, на который должен быть доставлен файл. Однако на более низком уровне протоколу требуется знать, куда направить порции данных, перемещаемые от отправителя к получателю, так что файл может быть корректно повторно собран при получении.

На стороне отправителя большая часть времени протокола уходит на разборку исходного сообщения на части, чтобы отправить их аккуратно и без потерь. На приемном конце ПО протокола расходует свое время на вскрытие упакованной информации и повторной сборки целого из частей. В ходе этого процесса отправитель и получатель также обмениваются информацией, предназначенной для того, чтобы следить за точностью и эффективностью их взаимодействия и определения момента завершения доставки. Протоколы также следят за качеством и эксплуатационной готовностью сетевых линий связи.

Если говорить коротко, отправка и получение сообщений в пределах сети требуют значительно большего объема взаимодействий и операций, чем пересылка почты из отправляющего почтового отделения в получающее. Однако почтовая аналогия остается весьма неплохим объяснением общего характера процесса (если не принимать во внимание рутинных процедур над внутренними сообщениями, выполняемых протоколом, но не почтовым отделением).

Семь уровней протоколов

Сетевые проколы группируются в соответствии с их функциями, такими как отправка и прием сообщений от сетевого интерфейса, взаимодействие с оборудованием, обеспечение работы приложений в их сетевом окружении и взаимодействие с ПО.

Эта групповая организация приводит к пакетированию нескольких уровней функций, при этом с каждым уровнем связано специфическое ПО. Когда в компьютер загружается ПО, поддерживающее конкретный сетевой протокол, оно называется *стеком протоколов*. Все компьютеры в сети загружают весь стек или его часть. Они используют одни и те же части стека, называемые *протоколами взаимодействия равноправных узлов,* когда они взаимодействуют друг с другом как (вы догадались!) равноправные узлы.

Самый широко известный набор сетевых протоколов разного уровня был разработан в 1980 году в ходе реализации международной программы под названием *OS! (Open System Interconnection — взаимодействие открытых систем).* Соответствующая модель сетевого взаимодействия известна как *эталонная модель взаимодействия открытых систем (OSI reference model)* (ее также часто называют просто моделью OSI), поскольку она определяет общую точку зрения, необходимую для понимания способа работы сетей. Хотя программа OSI в действительности не получила всеобщего признания, модель OSI остается стандартным средством объяснения структуры и поведения сетевого взаимодействия. Модель OSI показана на рис. 3.1.

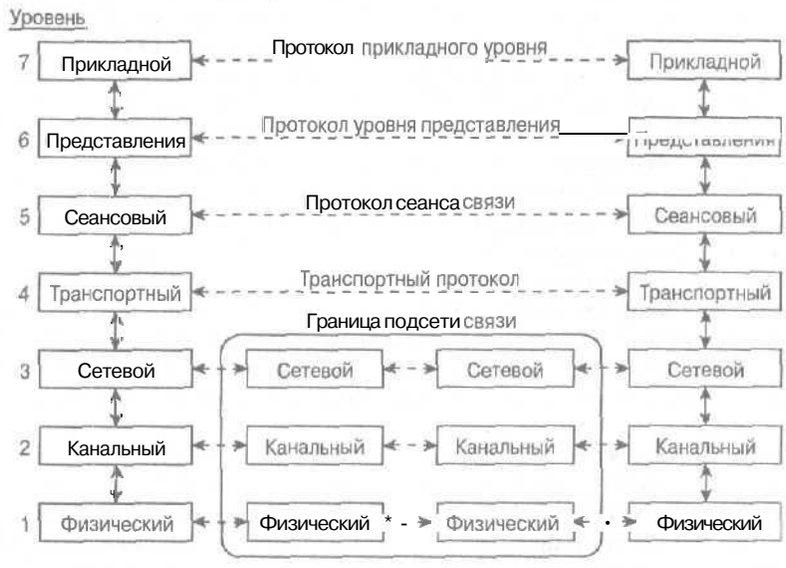


Рис. 3.1. Эталонная модель OSI разделяет сетевые протоколы на семь уровней

Модель OSI состоит из семи уровней, перечисленных ниже (уровни работают в обратном порядке).

- ✓ **Физический уровень (Physical layer).** Это уровень, на котором функционирует сетевое оборудование. Правила для этого уровня оперируют типом используемых коннекторов, типом метода подачи сигналов, которые переносят данные по сети, и типом кабеля или другой сетевой среды, которую использует физическая, материальная, часть сети. В некотором смысле это единственная часть модели OSI, которую можно увидеть и потрогать.
- ✓ **Уровень канала передачи данных (Data link layer).** Этот уровень оперирует взаимодействием с сетевым оборудованием, Для исходящих сообщений канальный уровень преобразует двоичные разряды, которые компьютеры используют для представления данных в эквивалентные сигналы, необходимые для перемещения данных по сети. Для входящих сообщений он осуществляет обратный процесс, преобразуя сигналы в их двоичный эквивалент. Канальный уровень также присутствует там, где идет обработка низкоуровневых адресов оборудования для отдельных сетевых карт и других устройств.

- ✓ **Сетевой уровень (Network layer).** Этот уровень направляет сообщения между отправителями и получателями; это означает, что он также управляет преобразованием сетевых адресов, удобных для восприятия человеком, в сетевые адреса, воспринимаемые компьютером (сетевые адреса не совпадают с адресами оборудования, которые обрабатывает канальный уровень). Каждое сообщение, проходящее через этот уровень, включает адреса отправителя и получателя для идентификации сторон, участвующих в обмене. Сетевой уровень перемещает данные от отправителя к получателю, когда и тот и другой не принадлежат одному кабельному сегменту.
- ✓ **Транспортный уровень (Transport layer).** Этот уровень дробит объемные сообщения на так называемые *протокольные блоки данных (Protocol Data Unit — PDU),* или пакеты, и отправляет их по сети. Он также собирает PDU в одно целое для восстановления сообщений по прибытии. Транспортный уровень может также включать проверки целостности данных с помощью добавления к каждому сообщению битовой комбинации, основанной на математических вычислениях, которые выполняются перед отправкой. Аналогичные вычисления повторяются отправителем, а результат сравнивается с предварительно вычисленным значением. Если оба значения совпадают, транспортный уровень предполагает, что передача была точной и корректной; если они не совпадают, транспортный уровень выдает запрос на повторную пересылку PDU. Эта функция проверки целостности необязательна; таким образом, некоторые протоколы транспортного уровня включают поверку целостности, а другие нет.
- ✓ **Сеансовый уровень (Session layer).** Этот уровень устанавливает текущий сетевой обмен сообщениями, называемый *сеансом (session),* между отправителем и получателем. Этот тип текущего соединения облегчает компьютерам обмен большими объемами данных либо поддержку соединения при регулярном перемещении данных между обеими сторонами для сеанса. Таким образом, сеансовый уровень управляет *установлением сеанса (session setup)* (которое аналогично набору телефонного номера), поддержкой сеанса *(session maintenance)* (которая аналогична ведению телефонного разговора) и завершением сеанса *(session termination),* или *разрывом* (teardown) (который аналогичен окончанию телефонного разговора и последующему отбою).
- ✓ **Уровень представления данных (Representation** layer). Этот уровень преобразует данные для доставки по сети. Эти операции преобразования выполняются в предположении, что отправитель и получатель могут не разделять общего набора типов данных, форматов и представлений. Таким образом, уровень представления данных преобразует данные из форматов, созданных отправителем, в общие форматы для передачи по сети, а затем при получении преобразует этот общий формат в формат, специфический для получателя. Этот процесс преобразования позволяет программистам по обе стороны сетевого соединения предполагать общие форматы для сетевых данных и более легко манипулировать деталями, необходимыми для доставки этих данных определенному клиенту.
- ✓ **Прикладной уровень (Application layer).** Название этого уровня служит примером неправильного употребления термина. Его нельзя отнести на счет приложения или службы, которым требуется отправить или принять данные в пределах сети. Скорее, оно относится к интерфейсу между стеком протоколов и приложениями или системными службами. Прикладной уровень определяет метод, посредством которого приложения или системные службы могут запрашивать доступ к сети и ко входящим данным, поступающим из сети.

Каждый из уровнен функционирует более-менее независимо от других. Однако задача каждого уровня состоит в том, чтобы обеспечить обслуживание вышележащего уровня и доставить данные нижележащему уровню. (Самый нижний уровень модели OSI, физический уровень, просто посылает данные получателю или уровню канала передачи данных, в зависимости от того, устанавливается связь или уже действует.)

Операции шифрования, которую выполняет уровень на передающей стороне, соответствует операция дешифрования, которую осуществляет тот же уровень на принимающей стороне. Таким образом, многоуровневая модель OSI помогает понять, что протоколы на передающем конце принимают данные от приложения, преобразуют эти данные в общую форму. управляют диалогом, подготавливают данные для отправки по сети, адресуют и маршрутизируют данные, а затем преобразуют их в сигналы для передачи по сети.

На принимающем конце процесс идет в обратном порядке: протоколы преобразуют сигналы в данные, вычисляют, куда эти данные должны быть доставлены, восстанавливают входящие сообщения в исходные контейнеры, управляют диалогом, подготавливают данные для клиентского компьютера и доставляют их приложению.

Некоторые не лишенные чувства юмора люди утверждают, что в стеке протоколов существует восьмой уровень и что он является самым важным. Он называется "политическим" или "религиозным" уровнем и в шутку относится к господствующим в организации мнениям и требованиям, которые выступают движущей силой в использовании сети. Хотя в модели OSI и не существует восьмого уровня, было бы весьма благоразумно иметь его в виду всякий раз, когда вы должны продвигать сетевую технологию среди высшего руководства вашей организации.

Протоколы Windows 2003 (и не только)

Подобно тому, как дипломатический протокол "смазывает колеса" международных отношений, сетевой протокол "вращает колеса" сети. Лучше узнав этих игроков на сетевом поле, вы глубже проникнете в сущность работы вашей сети. А в качестве вознаграждения будете также лучше подготовлены к решению сетевых проблем.

Windows Server 2003 включает поддержку двух основных наборов протоколов.

- ✓ **ТСРЛР (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Internet).** Набор стандартных протоколов и служб, разработанных по заказу правительства США в конце 1970-х–начале 1980-х годов. Сегодня ТСРЛР — самый широко используемый в мире комплект сетевых проколов.
- ✓ **IPX/SPX (Internet Packet eXchange/Sequenced Packet eXchange — межсетевой обмен пакетами/последовательный обмен пакетами).** Базовый протокол системы NetWare, разработанный в начале 1980-х годов.

Windows Server 2003 также включает встроенную поддержку нескольких специальных протоколов. К ним относятся *AppleTalk*— собственный сетевой протокол ОС Macintosh, а также Reliable Multicast Protocol (надежный многоадресный протокол) — сетевой протокол, используемый для повышения качества передачи данных одновременно нескольким приемникам.

В вашей сети вы можете использовать один или нескольких протоколов, которые несут сетям Windows 2003 как благо, так и беду. В следующих разделах мы рассмотрим каждый из названных протоколов и поясним, когда и почему вам может потребоваться использовать их. Не беспокойтесь, если встретите незнакомые аббревиатуры или кажущиеся странными термины; сконцентрируйтесь на выяснении того, как протоколы работают при подключении программ и служб к вашей сети (и к вашим сетевым пользователям). Уяснив эти понятия, вы овладеете действительно важными вещами.

TCP/IP - набор для Internet

Протокол TCP/IP появился в ходе исследования, финансируемого Министерством обороны США, начало которого относится к 1970-м годам, когда федеральные власти осознали, что им требуется технология, которая помогла бы связать все разнородные компьютерные системы в единую сеть. Иногда протоколы пакета TCP/IP называют *DoD-протоколами* (Department of Defense — Министерство обороны), поскольку Министерство обороны требовало, чтобы все приобретаемые им компьютеры могли использовать его. Протоколы TCP/IP также называют *Internet-протоколами*, так как они составляют основу, на которой функционирует Internet.

TCP/IP — это фактически аббревиатура для двух членов набора протоколов: протокола управления передачей (TCP) и протокола Internet (IP). Согласно высказыванию д-ра Винтона Серфа (Vinton Cerf), одного из основоположников технологии Internet, более миллиона сетей составляют часть собственно Internet, но равное количество (или даже больше) частных сетей также используют Internet.

Внимание, аббревиатуры!

Для поиска и устранения неисправностей в сетях Windows 2003 вам необходимо понимать, что делают различные протоколы, чтобы со знанием дела судить о тех проблемах, которые может породить каждый из них. В процессе работы с этими протоколами вам придется научиться жонглировать неудобными буквенно-цифровыми агрегатами ~ аббревиатурами и сокращениями.

Вы должны знать, какие аббревиатуры подходят друг другу и как фрагменты различных стеков протоколов "стыкуются" между собой. В случае разного рода инцидентов (а мы должны с сожалением заметить, что время от времени они случаются) вы должны знать о "фотогалерее" ненадежных протоколов Windows 2003, чтобы уметь выявить их.

Большинство названий протоколов изобилует аббревиатурами и сокращениями. Смиритесь с этим фактом в дальнейшем это пригодится вам.

Протокол TCP/IP получил наиболее широкое распространение среди всех сетевых протоколов — он охватывает около 100 миллионов пользователей во всем мире. Протокол TCP/IP также глубоко укоренился среди пользователей UNIX-систем благодаря его включению в начале 1980-х годов в общедоступную версию бесплатной системы BSD UNIX (Berkeley Software Distribution UNIX — ОС семейства UNIX, разработанная в лабораториях Беркли, Калифорнийский университет). Вскоре после этого он также был включен в официальную версию UNIX от AT&T/Bell Labs.

Поскольку протокол TCP/IP был разработан с целью обеспечения возможности связи и взаимодействия разнородных компьютеров, он работает на большем количестве типов аппаратных платформ, чем любой другой протокол. Поэтому вы не должны удивляться, что большинство коммерческих операционных систем, в то числе Windows, Macintosh и UNIX, включает встроенные реализации TCP/IP.

В настоящее время используются две версии TCP/IP. Версия 4 базируется на 32-разрядной схеме адресации. Именно эта версия TCP/IP используется по умолчанию в Windows 2003, а также в предыдущих версиях ОС Microsoft Windows, способных работать с сетью. TCP/IP версии 6 базируется на 128-разрядной схеме адресации. TCP/IP версии 4 используется настолько широко, что почти все возможные адреса уже отведены некоторым системам. Чтобы разрешить эту проблему, был разработан ряд технологий (таких как частные IP-адреса, для которых нельзя использовать маршрутизацию, или использование модулей доступа (proxy-систем) трансляции сетевых адресов (network address translation — NAT) для скрытия внут-

ренних сетевых адресов от Internet), но столпотворение вокруг IP-адресов от этого не уменьшилось. Версия 6 протокола TCP/IP допускает такое большое количество адресов, что каждому человеку на планете можно выделить 4,86 x 10^{28} IP-адресов (это просто невообразимое количество).

Windows Server 2003 может использовать TCP/IP версии 6, если вы установите ее (то же справедливо для Windows 2000 и Windows XP). Однако вы сможете ее использовать только в пределах частной сети или при подключении к I2 (абсолютно новая, высокоскоростная, сверхсовременная версия Internet, доступ к которой в США имеют только правительственные, военные и научные организации).

Поскольку TCP/IP составляет основу Internet и является наиболее широко используемым протоколом, мы рассматриваем его стандартный, применяемый по умолчанию, протокол для большинства сетей. Хотя изучение и использование TCP/IP — непростое дело, он обеспечивает больше функций и возможностей, чем любой другой протокол. Фактически компания Microsoft рекомендует TCP/IP как наилучший протокол для использования в Windows Server 2003.

IPX/SPX - оригинальный протокол NetWare

Протоколы *IPX (Internetwork Packet Exchange — межсетевой пакетный обмен), SPX (sequenced packet exchange — упорядоченный обмен пакетами)* и *NCP (NetWare Core Protocol — протокол ядра Netware)* представляют собой оригинальные протоколы системы NetWare компании Novell. Протоколы IPX, SPX и NCP, которыми пользуются 48 миллионов пользователей, относятся к наиболее широко используемым сетевым протоколам в мире. Вы можете использовать протокол IPX с системой NetWare для различных ОС, включая DOS, Windows *3x*, Windows *9x*, Windows 2000, Windows XP, Windows Server 2003, Macintosh, OS/2 и некоторые разновидности UNIX.

Обычно этот протокол требуется только в случае использования в сети NetWare 4.0 или более старых версий этой ОС. Начиная с версии NetWare 5.0 компания Novell обеспечивает собственную поддержку TCPЛP, так что мы ожидаем уменьшения использования IPX/SPX с течением времени. Пожалуйста, обратите внимание, что поскольку Microsoft не желает платить Novell за использование торговой марки IPX/SPX, Microsoft использует IPX/SPX под именем NWLink. (В Windows *9x* он называется IPX/SPX-совместимым протоколом.)

IPX/SPX — удобный протокол с развитыми возможностями маршрутизации, поэтому он работает в сетях любого масштаба. Однако использование IPX/SPX предполагает наличие в сети сервера NetWare 4.0 (или более старой версии). Вы можете со временем отучиться от этого протокола или вообще отказаться от него из-за перехода вашей организации к протоколу TCPЛP, протоколу Internet, с которым IPX/SPX несовместим.

Другие лица, другие протоколы

В сети, с которой вы работаете, могут неожиданно обнаружиться другие, менее распространенные протоколы, например, из приведенного ниже списка.

1 ✓ **DLC (Data Link Protocol — протокол управления каналом передачи данных).** Устаревший протокол, используемый для подключения сетевых принтеров и некоторых мэйнфреймов компании ЮМ. Этот протокол исключен их операционных систем Microsoft. Он был без особого шума заявлен в Windows 2000, но напрочь изъят из Windows XP и Windows Server 2003. Если вам требуется доступ к сетевому принтеру, вы, скоре всего, воспользуетесь протоколом TCPЛP либо собственным протоколом от

изготовителя принтера. Аналогично, если вам необходима связь с мэйфреймами или другими чрезвычайно устаревшими системами, вы можете воспользоваться протоколом TCP/IP, шлюзом или протоколом от изготовителя. Протокол DLC по-прежнему может использоваться в системе Windows Server 2003, однако вам необходимо найти стороннего поставщика, который обеспечит установочный диск, поскольку Microsoft не включила его в пакет поставки (т.е. в компакт-диск с дистрибуцией).

- ✓ **NetBIOS (Network Basic Input/Output System — сетевая базовая система ввода-вывода).** Сетевой протокол NetBIOS — это API-интерфейс, разработанный фирмой ЮМ и доработанный Microsoft. NetBIOS наряду с NetBEUI формирует исходные сетевые компоненты для систем LAN Manager и Windows NT. Протокол NetBIOS также работает с протоколами IPX/SPX и TCP/IP, поэтому не следует думать, что NetBIOS требует NetBEUI. (Это не так.) Если вы работаете с сетью только с использованием систем Windows 2000, Windows XP и Windows Server 2003, вы можете вообще не использовать NetBIOS!
- ✓ **NetBEUI (Extended User Interface — расширенный интерфейс пользователя NetBIOS).** NetBEUI — скоростной, эффективный, но не допускающий маршрутизации протокол транспортного уровня для локальных сетей, разработанный фирмой IBM и доработанный Microsoft. NetBEUI и NetBIOS были исходными сетевыми компонентами для систем LAN Manager и Windows NT. NetBEUI вымер подобно мамонтам, по крайней мере, если судить по Windows XP и Windows Server 2003. NetBEUI можно по-прежнему использовать в системе Windows Server 2003, но вам потребуется найти стороннего поставщика, чтобы получить установочный диск.
- ✓ **Apple Talk.** Название набора протоколов, созданных компанией Apple Computer, чей компьютер Macintosh был одним из первых массовых компьютеров, включающих встроенное сетевое аппаратное и программное обеспечение. В большинстве случаев у владельцев компьютеров Macintosh возникает потребность в стеке протоколов Apple Talk. Чтобы предоставить доступ к файлам и службе печати клиентам Macintosh, компания Microsoft включила сетевой компонент под названием Service for Macintosh. Этот модуль надстройки (который не устанавливается во время начальной установки Windows Server 2003) позволяет пользователям Macintosh осуществлять доступ к файлам, принтерам или службам Windows Server 2003.
- ✓ ISO/OSI. Забавный палиндром, за которым скрывается набор протоколов *взаимодействия открытых систем,* предложенный *Международной организацией по стандартизации (International Standards Organization/Open System Interconnection).* Модель ISO никогда не служила своей первоначальной цели — заменить TCP/IP. Некоторые OSI-протоколы широко используются в Европе, где они завоевали прочный плацдарм. Отсюда протоколы ISO проникают в индустрию, правительственные, научные и коммерческие организации, поскольку многие правительства, включая правительство США, требуют, чтобы компьютерные системы были OSI-совместимыми.

  Подобно TCP/IP, протоколы OSI доступны для широкого диапазона систем, начиная с ПК и заканчивая суперкомпьютерами. Большинство стеков протоколов для сетей имеет сходство с эталонной моделью OSI, и эта модель остается самым ценным наследием работ, которые восходят к созданию сетей на базе протоколов OSI в 1980-х годах. Реализация ISO/OSI для Windows 2003 предлагается многочисленными независимыми разработчиками, большую часть которых составляют европейские компании, но сама Microsoft не включает эти протоколы в свою ОС.

- ✓ **SNA (Systems Network Architecture — системная сетевая архитектура).** Это основной комплект протоколов фирмы IBM для доступа к крупномасштабным сетям и мэйнфреймам. Поскольку SNA был новаторским протоколом, многие компании, которые вкладывали значительные средства в мэйнфреймы, обычно также вкладывали их в SNA. Многие сети SNA по-прежнему используются, но их количество уменьшается, поскольку SNA — устаревший, громоздкий и дорогой протокол, и, кроме того, TCP/IP отбирает "хлеб" у OSI, даже на мэйнфреймах.

Классификация протоколов по типу соединений

Протоколы IP, IPX и NetBEUI относятся к протоколам сетевого взаимодействия ***без подтверждения соединения (connectionless),*** протоколы SPX и TCP — к протоколам сетевого взаимодействия ***ориентированным на соединение*** *(connection-oriented).* Что это значит? И стоит ли вам беспокоиться?

Все названные протоколы работают на нижнем уровне. Ранее а этой главе мы рассказали о том, что самая важная задача протоколов нижнего уровня состоит в разбиении сообщений произвольной длины на "удобоваримые" порции при отсылке данных по сети с последующим восстановлением общего из частей при получении. Эти порции, называемые *пакетами,* формируют базовые блоки сообщений для данных, перемещаемых по сети. Эти пакеты подвергаются дальнейшему делению и помещаются в свои конверты с помощью соответствующего метода доступа. Подобные конверты называются ***кадрами (frame).*** На это можно посмотреть таким образом: пакеты снуют вверх-вниз по стеку протоколов, а кадры, "пританцовывая", идут по кабелям.

Протоколы без подтверждения соединения работают аналогично пересылке писем через почтовую службу. Вы бросаете письмо в почтовый ящик и рассчитываете на то, что почта доставит его. Вы можете никогда не узнать, действительно ли письмо дошло, — если только это не счет! Протоколы IP, IPX и NetBEUI не дают гарантий доставки, а кадры могут приходить в любом порядке.

С другой стороны, протоколы ориентированные на соединение для начала взаимодействия используют так называемое квитирование установления связи, или просто подтверждение связи. При этом потенциальный отправитель перед началом отправки спрашивает получателя, может ли тот принять входное сообщение. После начала передачи протоколы ориентированные на соединение трактуют каждое сообщение как заказное письмо» когда вы получаете обратную квитанцию, подтверждающую его получение. Пакеты протоколов SPX и TCP упорядочены таким образом, что после получения **их** можно восстановить в первоначальной последовательности, что делает их более надежными. Протоколы ориентированные на соединение могут также запрашивать повторную доставку или отправку уведомления об ошибке, когда пакеты повреждены или утеряны по пути от отправителя к получателю.

IP и другие протоколы, без подтверждения соединения обычно работают быстрее и требуют небольших накладных расходов, но их рассматривают как упрощенные и ненадежные. TCP и другие протоколы, ориентированные на соединение, работают более медленно, чем их не ориентированные на соединение двойники, поскольку следят за тем, что было отправлено и получено, наблюдают, таким образом, за состоянием соединения между отравителем и получателем. В каждый пакет помещается большой объем информации для ведения записей и проверки данных, что увеличивает требования к накладным расходам, но одновременно повышает надежность.

В мире сетей существуют сотни наборов протоколов, каждый из которых обладает собственными аббревиатурами и специальными возможностями, но вам нет необходимости знать большинство из них. Если в этой главе вы не встретили названия протокола, который работает в вашей сети, вы, вероятно, знаете о нем больше, чем мы можем вам рассказать.

Совмещение протоколов

Иногда вам может потребоваться использовать на вашем компьютере больше одного сетевого протокола. Это может подчас потребовать от вас некоторой изворотливости, но Windows Server 2003 приспособлен для поддержки нескольких протоколов. В действительности вы мо-

жете запустить и TCP/IP, и IPX/SPX (NWLink) (плюс любой другой "родной" протокол или протокол от стороннего поставщика) на одной машине, работающей под управлением Windows Server 2003, для нескольких сетевых адаптеров без особых трудностей. То же справедливо для систем Windows 98/Windows SE/Windows Me/Windows NT/Windows 2000 и Windows XP.

Аналогично, компьютеры Macintosh могут легко совместно использовать протоколы AppleTalk и TCP/IP, а UNIX может запускать столько стеков протоколов, сколько вам может потребоваться для получения необходимого спектра сетевых услуг. Набор протоколов UNIX-машины может включать такие протоколы, как TCP/IP, NetBEUI, OSI, IPX и др.

Может случиться, что вашей самой большой проблемой станет использование нескольких стеков протоколов на устаревшей модели ПК, функционирующей под управлением DOS или Windows 3.x, где отсутствие встроенных сетевых возможностей автоматически приводит к более трудной установке и использованию нескольких протоколов. Также ограниченные возможности управления памятью и отсутствие поддержки драйверов для современных устройств могут привести к проблемам при создании многопротокольной сети.

Посмотрим, что там if вас на сервере

С помощью Windows Server 2003 можно легко проверить, какие протоколы установлены на вашей машине. Следует просто запустить утилиту Network Connections (для этого выполните команду Start⇨Control Panel (Пуск⇨Панель управления), щелкните правой кнопкой мыши на пункте меню Network Connections (Сетевые подключения) и выберите пункт Open (Открыть)). Затем щелкните на меню Advanced (Дополнительно) и выберите пункт Advanced Settings (Дополнительные параметры). Результат этих действий показан на рис. 3.2.

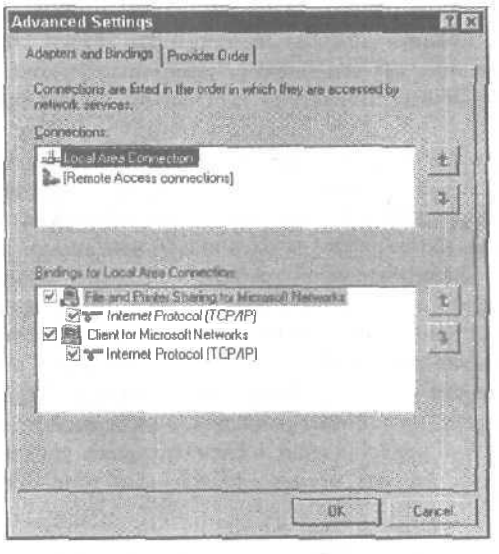


Рис. 3.2. Проверка наличия установленных протоколов

На рис. 3.2 видно, что из всего изученного в этой главе мы применяем в своей сети только протокол TCP/IP. (На рис. 3.2 также показано, что протокол TCP/IP связан со всеми службами, выявленными для нашего локального соединения.) Применительно к вашей сети вас должны интересовать только протоколы, которые появляются в этом окне (или протоколы, которые, как вы полагаете, должны отображаться, однако не отображаются, как это иногда бывает).

Глава 4

Полцарства за топологию!

В этой главе...

- Топология как соединение линий
- Знакомство с основными топологиями: "звезда", "шина", "кольцо"
- Комбинация топологий и связывание сетей
- Знакомство с сетевыми топологиями
- Введение в базовые топологии: Ethernet, Token Ring и др.
- Межсетевое оборудование: повторители, маршрутизаторы, мосты, мосты-маршрутизаторы и шлюзы

Когда математики собираются вместе, они не находят лучшего развлечения, чем придумывание новых терминов, чтобы сбить с толку всех остальных. (Может, им не хочется, чтобы ученые в области вычислительной техники монополизировали "рынок" непонятной терминологии.) Термин *топология* (*topology*) пришел в компьютерные сети из математики; топология описывает способ, которым компьютеры связаны между собой сетевой проводкой. Помимо способности напускать туману, топология дает краткий и точный способ описания того, как соединяются различные фрагменты и части сети. В этой главе мы расскажем о различных топологиях, которые вы сможете комбинировать при создании сети.

Однако проектирование сети не сводится только к вопросам топологии. Вам также следует рассмотреть использование специального оборудования и способы взаимодействия этого оборудования с другим оборудованием — *аппаратную реализацию,* если вам угодно.

Видимо, из зависти к математикам и их способности выдумывать "крутые" термины, группа специалистов по вычислительной технике придумала термин *сетевые технологии,* чтобы обозначить специфическое оборудование и методы передачи сигналов, используемые в сетях. Из зависти к этой группе специалистов по вычислительной технике другая группа решила, что более продуктивно представлять это же оборудование и методы передачи сигналов в терминах *методов доступа* — способа мышления, который в большей степени концентрируется на том, как оборудование получает разрешение на передачу сигналов по сетевой среде.

Эта глава также даст вам представление о специфических аппаратных реализациях, сетевых технологиях и методах доступа, которые превращают топологию в реальную, работающую сеть.

Что такое топология

На языке математики топология — это расположение линий между точками *в* графе. Применительно к сетям слово *топология* относится к способу, которым провода (линии) протягиваются между компьютерами (точками графа). Поэтому, когда вы слышите слово *топология* на конференции, посвященной сетям, речь идет о расположении компьютеров в сети.

Сетевую проводку (или кабельную систему) можно проложить разными способами. На рис. 4.1 показаны две наиболее распространенные схемы — топология типа "звезда" и топология типа "шина". Существует еще одна распространенная схема, называемая *кольцевой топологией,* при которой сетевая проводка делается по образцу окружности, когда последний компьютер в кольце соединяется с первым.

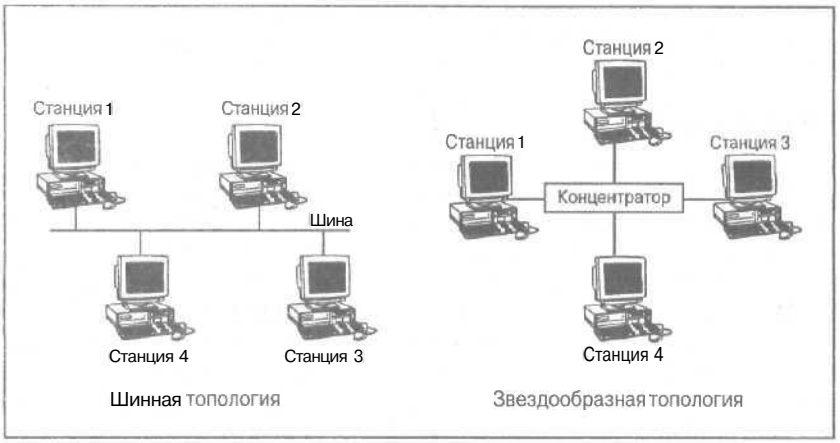


Рис. 4.1. Схемы "звезда" и "шина" часто встречаются вместе

Топологии могут комбинироваться многими интересными способами. Если, для того чтобы связать вместе несколько отдельных "звезд", вы используете "шину", то в результате вы получите *сеть* типа *распределенной звезды,* известную также как *гибридная сеть.* Большая часть сетей является некоторыми гибридами, но, в общем, чем проще топология, тем лучше работает сеть.

Звезда сетевого мира

Звездообразная топология состоит из отдельных проводов, которые исходят из центральной точки — обычно подключенной к отдельному устройству, называемому *концентратором (hub)* (о концентраторах речь пойдет ниже в этой главе), — к отдельным устройствам, подключенным к другому концу каждого провода. *Шинная топология* представляет собой единый кабель, к которому подключены все устройства сети (или некоторой части сети, что встречается чаще).

Если в сети со звездообразной топологией разорвать один из проводов, это скажется только на одном звене, а все остальное будет продолжать работать. Если разорвать провод в сети с шинной топологией, то все, что подсоединено к этой шине, теряет способность доступа к сети.

В звездообразной топологии концентратор в центре "звезды" действует в качестве реле для компьютеров, подключенных к ее лучам, следующим образом.

1. Компьютер-отправитель посылает порцию данных по сетевому кабелю, предназначенную некоторому сетевому компьютеру.
2. Концентратор, находящийся между отправителем и получателем, пропускает сообщение к компьютеру-адресату (если он подключен к тому же концентратору) либо к некоторому другому концентратору или сетевому устройству, если он не присоединен к тому же самому концентратору.

3. Концентратор, к которому подключен компьютер-адресат, отправляет сообщение этому компьютеру (в предположении, что отправитель и получатель принадлежат топологии типа "звезда", однако ничто не препятствует сетевому обмену в рамках разных топологий, если только между ними существует корректный тип связи).

Применительно к большим сетям средний шаг может повторяться несколько раз, по мере того, как данные переходят от отправителя к концентратору и получателю или от концентратора в шину, затем снова в концентратор и т.д., до тех пор, пока данные постепенно не достигают компьютера, которому они предназначены.

Оседлаем шину!

В сети с шинной топологией каждый компьютер, подключенный к одному и тому же кабелю, видит каждое сообщение, которое перемещается по этому кабелю. Если отправитель и получатель находятся на одном кабеле, называемом *сегментом,* сообщения перемещаются быстро. Если отправитель и получатель не находятся на одной шине, специальный компьютер пересылки, называемый мостом или маршрутизатором, пропускает сообщение из шины отправителя по направлению к шине получателя за счет копирования сообщения и его ретрансляции.

Мосты и маршрутизаторы рассматриваются более подробно ниже в этой главе. Здесь же представим *мост (bridge)* как устройство, которое переправляет информацию из одной сети в другую, пользуясь для этой цели адресами MAC-уровня *(Media Access Control — управление доступом к среде).* (MAC-адрес — это уникальное 48-разрядное число, присваиваемое сетевому адаптеру производителем; является физическим адресом; используется для отображения в сетях TCP/IP. — *Прим. перев.*) С другой стороны, маршрутизатор направляет информацию из одной сети в другую, пользуясь сетевыми адресами.

Аналогично тому, как вы можете пересылать сообщение через несколько концентраторов в сети типа "звезда", вы можете пересылать сообщение через несколько мостов или маршрутизаторов в сети с шинной топологией.

Посыльный бегает по кругу

Нам осталось рассмотреть еще одну основную топологию — кольцевую. Сети с чисто кольцевой топологией создаются нечасто, поскольку при разрыве кабеля они полностью выходят из строя. Вот почему сетевые технологии наподобие спецификации *FDDI (Fiber Distributed Data Interface — распределенный интерфейс передачи данных по волоконно-оптическим каналам*) используют чисто кольцевую топологию, которая включает сдвоенный кабель и отказоустойчивую схему, обеспечивающую восстановление сети после разрыва одного из кабелей.

Фактически большинство так называемых кольцевых топологий в действительности представляет собой сети, соединенные по схеме "звезда" или "шина", в которых логическая кольцевая структура накладывается на физическое соединение, в то время как ее реальная топология может быть звездообразной или шинной. Поэтому вы можете обнаружить, что сетевые технологии наподобие ARCnet *(Attached Resources Computing Net — вычислительная сеть с подключенными ресурсами* (сетевая архитектура корпорации Datapoint)) поддерживают логические кольцевые структуры поверх физических сетей со схемой "звезда" или "шина", а другие технологии наподобие Token Ring ("эстафетное кольцо" или "кольцевая сеть с маркером") поддерживают логическое "кольцо" поверх звездообразной сети (или распределенных звездообразных сетей). Эти структуры показаны на рис. 4.2.

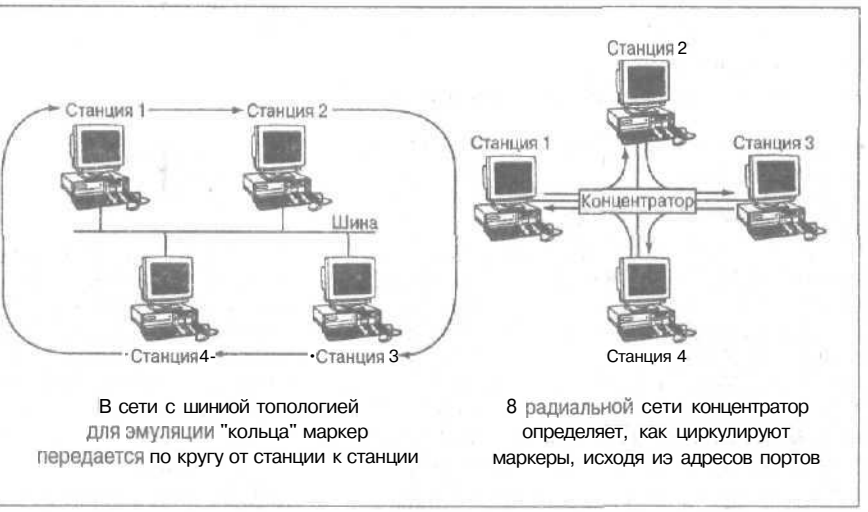


Рис. 4.2. Физическая "звезда" или "шина" может поддерживать логическое "кольцо"

Физическая и логическая

Сетевая топология может быть физической и логической. Физическая топология кольцевой сети с маркером — обычно радиальная, однако данные перемешаются от одного компьютера к другому по кольцу. Сеть ARCnet может быть физической "шиной" или "звездой" (или некоторой комбинацией обеих], но логически она представляет собой "кольцо". Даже такая сеть, как Ethernet, не избежала этой путаницы. Когда сеть Ethernet соединена "шиной", она работает как "шина"; но когда Ethernet связана в виде "звезды", она все равно работает как "шина".

Кольцевые топологии привлекательны тем, что позволяют отследить, кто приступил к отправке сообщения, за счет постоянной циркуляции в сети электронной формы разрешения на передачу, также известной как *маркер*. Только компьютер, владеющий маркером, может передавать сообщение в сеть, что исключает любую возможность одновременной попытки двух компьютеров отправить сообщения. В среднем каждый компьютер ожидает прихода маркера приблизительно в течение одного и того же промежутка времени, поэтому в течение достаточно длительного интервала времени каждый компьютер получает равную квоту времени доступа к сети. Этот подход позволяет более полно использовать доступную полосу пропускания сети до того, как скорость работы сети снизится.

В своих рассуждениях о сетях не путайтесь в понятиях сетевой топологии и сетевой технологии. Топология определяет схему сетевой проводки, ясную и простую. Топология описывает, каким образом сообщения перемещаются между компьютерами и другими устройствами в сети. Сетевая технология, иногда называемая методом доступа, определяет поведение сети и необходимые типы интерфейса и оборудования. Поэтому сетевая технология также описывает с высокой степенью детализации физические характеристики сети, в том числе следующие.

- ✓ Электрические характеристики сети.
- ✓ Используемый сетью тип сигналов.
- ✓ Тип используемых сетью коннекторов.

- ✓ Типы интерфейсов и способы их совместной работы.
- ✓ Максимальный объем сообщений.
- ✓ Другие характеристики, необходимые для создания сети.

Больше чем маркер

Для организации взаимодействия компьютеров сети используют наборы правил, называемые ***протоколами***. В некоторых сетях для управления этим взаимодействием используются ***маркеры (taken).*** В других сетевых технологиях выбор сделан в пользу общедоступности узлов, и любой компьютер может отправить данные любому незанятому узлу. Сети, которые посылают маркеры, называются **сетями с *маркерным доступом* (или сетями с** эстафетной ***передачей маркера — token-passing network)***. Они используют для управления доступом к сети протоколы с маркерным доступом. Это значит, что для передачи данных они должны ждать прихода подходящего маркера.

Для сетей с открытым доступом все выглядит несколько сложнее: компьютеры должны прослушивать среду, чтобы определить, используется ли она в текущий момент (на что указывают активные сигналы в среде). Если компьютеру необходимо осуществить передачу, он останавливается и слушает, чтобы понять, "говорит" ли кто-j нибудь еще. Если компьютер не слышит никаких сигналов, он может "выйти вперед" и тотчас начать передачу. Когда другой компьютер проделывает то же самое приблизительно в то же самое время, данные от одного из компьютеров "сталкиваются" с данными от другого и оба компьютера должны отступить и повторить попытку.

Естественно, вам требуется что-нибудь более приемлемое, что позволило бы избежать подобного рода конфликтов. Сеть Ethernet реализует метод ***CSMA/CD*** *(Carrier* ***Sense Multiple Access*** *with* ***Collision Avoidance*** *— множественный доступ* ***с контролем несущей*** **и предотвращением** ***конфликтов)***, в то время как сети ARCnet и token-ring реализуют протоколы с маркерным доступом. Описания того, как эти технологии осуществляют доступ к сетевой среде, называются ***методами*** доступа ***(access method)***. Многие часто путают топологии с методами доступа или сетевыми технологиями, но теперь, когда мы выявили источник этой путаницы, детали различных сетевых технологий, описанных в этой главе, должны быть истолкованы верно.

Топология касается схемы сети, а сетевая технология (или метод доступа) — способа функционирования сети. Иначе говоря, топология обозначает используемую схему кабельной разводки, а сетевая технология определяет, какие физические компоненты вам необходимо приобрести, чтобы эта схема работала.

Азбука сетевой технологии

Все имеющиеся на сегодняшний день на рынке сетевые технологии можно разделить на пять категорий. Поэтому, ответив на все пять следующих вопросов, вы сможете отличить один тип сетевой технологии от другого.

- ✓ Какой метод доступа, протокол и топологию использует сеть?
- ✓ Как работает сеть?
- ✓ Какими техническими преимуществами и недостатками обладает сеть?
- ✓ Какие типы сетевых сред поддерживает сеть?
- ✓ Какова коммерческая привлекательность сети (стоимость, доступность и т.д.)?

В следующих разделах мы рассмотрим аргументы "за" и "против", касающиеся различных сетевых технологий, — с точки зрения того, как именно вы должны действовать, когда вам необходимо применить некоторую технологию к конкретной топологии с целью наилучшего обслуживания запросов ваших пользователей.

В соревновании технологий участвуют...

Когда вы говорите о сетевых технологиях, вы говорите о специфическом типе оборудования и связанных с ним программных драйверах, которые, будучи установлены в ПК, могут порождать работающее сетевое соединение. Рабочая часть, впрочем, зависит от правильно выбранной инфраструктуры — кабелей, соединений и вспомогательного оборудования (наподобие мостов и маршрутизаторов).

Для целей этой книги мы выбрали две основные сетевые технологии (с учетом многочисленных упрощений, как станет ясно позже).

- ✓ Ethernet.
- ✓ Token Ring.
- ✓ Другие.

Конечно, вы поймали нас на попытке провести тайком третий, "сборный" пункт (мы едва не назвали его "*разное*"),чтобы дать нам возможность кое-что сказать о некоторых из многочисленных доступных (но менее распространенных) сетевых технологиях, которые мы решили не рассматривать столь подробно в этой книге. В действительности недавний анализ отрасли показал, что с вероятностью около 75% ваша сеть использует (или будет использовать) одну или две первые сетевые технологии, упомянутые в предыдущем списке. Поэтому, хотя мы подробно рассматриваем только небольшое количество технологий, мы до некоторой степени охватываем большую часть сетей.

Познакомьтесь с Ethernet - самой популярной сетевой технологией

Ethernet — наиболее известная, широко используемая, универсальная сетевая технология, которую можно без труда приобрести. Ethernet существует дольше большинства других сетевых технологий, начиная со второй половины 1970-х годов. Ethernet была создана в исследовательском центре компании Xerox в Пало-Альто и позднее принята на вооружение такими компаниями, как Digital Equipment, Intel и Xerox (вот почему 15-контактные коннекторы для ThickWare Ethernet иногда называли *DIX*). Долгое время Ethernet играла роль сетевого продукта; это означает, что многочисленные поставщики присутствовали на этом рынке и что эта технология отличается широким спектром возможностей и вариантов выбора.

Ethernet использует метод доступа CSMA/CD. В приведенной ниже врезке "Ethernet: о важности бампера на битком забитых дорогах сети" объясняется, что эта штука означает на обычном языке, конечно, в той мере, в какой предмет это позволяет, — а это, увы, не так уж много.

Самый простой способ описания метода доступа CSMA/CD выглядит следующим образом: "Слушать, прежде чем отправить. Слушать при отправке. Если попадается мусор, прекратить отправку и попробовать снова позже".

Сильные и слабые стороны Ethernet

Технология Ethernet обладает следующими сильными сторонами: она надежна и существует в широком диапазоне вариантов, приемлемых технически и доступных по цене. К слабым сторонам Ethernet относятся неизбежность конфликтов и более трудные методы устранения проблем по сравнению с теми, которых требует шинная топология. Если рассматривать шкалу скоростей современных сетей, то базовая скорость сетей Ethernet, составляющая 10 Мбит/с (сокращение от *миллион бит в секунду),* приходится на ее "медленный" конец, однако сегодня доступна масса высокоскоростных версий Ethernet. (Более подробно мы остановимся на этом в главе 7.)

Ethernet не слишком хорошо работает с приложениями, отличающимися высокой загрузкой сети, и в тех случаях, когда необходима доставка данных в реальном времени (для видео и мультимедиа). Кроме того, Ethernet не отличается плавным понижением производительности в случае увеличения объемов трафика. Фактически с учетом метода доступа CSMA/CD эффективный потолок ее пропускной способности составляет 56–60% общей пропускной способности (или 5,5–6,0 Мбит/с для Ethernet со скоростью передачи 10 Мбит/с). Это уровень использования, при превышении которого рост вероятности конфликтов зачастую приводит к замедлению или полному отказу работы сети.

Ethernet: о важности бампера на битком забитых дорогах сети

Аббревиатура, которая описывает метод доступа Ethernet к среде, выглядит как CSMA/CD (Carrier Sense Multiple Access with Collision Avoidance — множественный доступ с контролем несущей и предотвращением конфликтов). (Слуховым эквивалентом конфликта является эхо.) При возникновении конфликта вы должны повторить передачу. Ниже приведены определения каждого термина, входящего в название метода.

- **Контроль несущей.** Все оборудование, подключенное к сети, всегда прослушивает кабель, и никто не может отправить сообщения, если это делает кто-то другой. Когда сообщение перемещается по кабелю, используется электрический сигнал, который называется ***сигналом несущей*** *частоты.* Прослушивая кабель, устройство знает, когда он занят, поскольку контролирует присутствие сигнала несущей частоты.
- **Множественный доступ.** Любое устройство, присоединенное к сети, может отправить сообщение, если только в этот момент не обнаружено присутствие сигнала несущей частоты. Это значит, что множественные отправители могут начать (и иногда начинают) отправку практически одновременно (когда они думают, что все спокойно), вот почему это называется ***множественным доступом.***
- **Предотвращение** конфликтов. Если два или несколько отправителей начинают передачу приблизительно в одно и то же время, рано или поздно их сообщения столкнутся друг с другом, вызвав ***конфликт.*** Конфликты легко распознать, поскольку они порождают "мусор" (ненужные данные), который совершенно не похож на правильную передачу. Аппаратура Ethernet включает схемы ***обнаружения*** **конфликтов** столкновений, которые при обнаружении конфликта немедленно прекращают передачу. При возникновении конфликта каждый отправитель ожидает случайный интервал времени, прежде чем начнет прослушивать кабель, чтобы повторить свою попытку передачи.

При планировании потребляемой пропускной способности для сети Ethernet ориентируйтесь на 55% общей пропускной способности (5,5 Мбит/с для 10-мегабитовой сети, 55 Мбит/с — для 100-мегабитовой сети и т.д.) как на практический потолок пропускной способности для любого сегмента сети. Если при проектировании сети вы планируете использовать пропускную способность Ethernet на полную мощность, в процессе эксплуатации такой сети вы рискуете столкнуться с проблемами.

Сегодня не существует ограничений на пропускную способность, которую предоставляет в распоряжение пользователей Ethernet. Большинство новых сетевых карт Ethernet имеют конструкцию "10/100"; это означает, что они применимы для 10- и 100-мегабитовых сетей Ethernet и подстраивают свою скорость соответствующим образом. Сегодня Gigabit Ethernet с его ошеломляющей общей теоретически достижимой пропускной способностью в 1000 Мбит/с поднимает потолок производительности сети на новую высоту и при этом сохраняет совместимость с другими версиями Ethernet.

Ethernet во всем разнообразии

Ethernet поставляется в огромном количестве разнообразных модификаций. Это значит, что Ethernet функционирует на любом из основных типов сетевых сред — витые пары, коаксиальные кабели (фактически целый ряд версий) и оптоволоконные кабели — и работает как с шинной, так и со звездообразной топологией. Один необычный вариант — 100BaseVG-AnyLAN — использует отличный от CSMA/CD метод доступа, называемый *приоритетом по запросу (demand priority),* который наделяет эту реализацию интересными особенностями. (Версия 100BaseVG-AnyLAN подробно описывается в главе 7.)

Вы также можете без труда найти Ethernet-устройства, которые позволяют комбинировать и совмещать среды; так что вы можете использовать Ethernet для создания сетей практически любого масштаба, работающих даже в наиболее неблагоприятных средах, таких как заводские цехи и машинные залы, где многочисленное тяжелое оборудование может создавать большие помехи).

Кроме того, технологии Ethernet поддерживают некоторые новейшие методы использования пропускной способности, так что вы случайно можете услышать о разновидностях Ethernet наподобие коммутируемой Ethernet (switched Ethernet) или полнодуплексной Ethernet (full-duplex Ethernet). Первая разновидность зависит от специального типа устройства (называемого, естественно, коммутатором), которое позволяет любым двум узлам устанавливать частное сквозное соединение. Таким образом, коммутируемая Ethernet позволяет парам машин использовать всю пропускную способность сетевой среды. (Это отличный способ продлить жизнь 10-мегабитовым Ethernet-системам.) Полнодуплексная Ethernet ограничена версией 100Base VG-AnyLAN и использует две пары кабелей, поэтому машины могут отправлять и получать данные одновременно, удваивая, таким образом, общую пропускную способность.

Коммерческая сторона Ethernet

Несмотря на свой "почтенный" возраст, Ethernet остается наиболее широко распространенной и популярной сетевой технологией. Среди основных доступных для Ethernet типов сред витая пара лидирует по количеству вновь устанавливаемых систем, однако в использовании попрежнему остается огромное количество систем на основе коаксиального кабеля. Ethernet-системы на основе волоконной оптики ограничены сетями масштаба кампуса, где наибольшее значение имеют вопросы больших расстояний и электрических помех. Однако они также используются в неблагоприятных средах и для приложений, требующих большой пропускной способности, включая реализации, поддерживающие скорости как 100 Мбит/с, так и 1 Гбит/с.

К основным причинам непоколебимой популярности Ethernet можно отнести следующие.

- ✓ **Приемлемая** цена. Кабели довольны дешевы, а стоимость плат сетевого интерфейса колеблегся от 20 долларов для базовых адаптеров до 200 долларов для мощных серверных адаптеров. Ethernet — не самая дешевая из всех сетевых технологий, но очень близка к этому!
- ✓ Свобода выбора. Ethernet поддерживает все типы сред, различную пропускную способность и огромное количество аппаратуры для создания гибридных сетей. Поставщики в изобилии предлагают оборудование для Ethernet. При возникновении необходимости в специализированном сетевом оборудовании или среде с высокой вероятностью именно для Ethernet найдутся подходящие альтернативы. Если какие-либо возможности сегодня недоступны, они скорее всего уже заложены в чьи-то новые проектные решения.
- ✓ **Опыт.** "Долгожительство" Ethernet означает, что найти специалистов по этой технологии нетрудно. Кроме того, огромный объем технических и учебных материалов по Ethernet позволяет относительно легко накопить необходимый опыт.

- ✓ **Постоянные нововведения.** Базовая технология Ethernet, обеспечивающая скорость 10 Мбит/с, — не чемпион по скорости. Однако поставщики изготавливают для Ethernet высокоскоростные коммутаторы, которые могут полностью предоставить эти 10 Мбит/с в распоряжение отдельных соединений; кроме того, всегда доступны и широко используются более скоростные разновидности Ethernet. По мере роста требований к пропускной способности инженеры находят способы усовершенствования возможностей Ethernet, которые бы удовлетворили эти требования, о чем свидетельствует, например, формализация технологии Gigabit Ethernet в качестве стандарта ШЕЕ 802.3Z.

Если перед вами стоит проблема создания новой сети и не существует каких-либо непреодолимых причин, диктующих выбор другой сетевой технологии, остановите свой выбор на Ethernet в силу всех означенных выше причин!

Примемся за Token Ring

Технология Token Ring завоевала прочное место на рынке, несмотря на то, что в коммерческом виде существует не так давно, как Ethernet. (Напомним читателям, что *технология Token Ring* — это технология кольцевых сетей с маркерным (эстафетным) доступом. Для краткости мы будем называть эту технологию **Token Ring.** — *Прим. перев.*) Технология Token Ring основана на технологии, которая была развита и первоначально выведена на рынок компанией IBM, так что ее обычно можно обнаружить в тех местах, где закрепилась ШМ. Когда место подключенных к мэйнфреймам ШМ неинтеллектуальных терминалов на столах стали занимать ПК, IBM начала действовать. Она разработала технологию Token Ring, чтобы привязать все эти новые ПК к своим большим машинам.

Технология Token Ring использует метод доступа с передачей маркера (token-passing) для совокупности отдельных двухточечных линий связи между парами устройств, расположенных по окружности. Термин *двухточечные (point-to-point)* означает, что одно устройство подключено непосредственно к другому. Для сети Token Ring термин "двухточечный" описывает соединение между компьютером и концентратором, который может быть подключен к другому концентратору или компьютеру. Хотя устройства, используемые в сетях Token Ring, работают подобно концентраторам, более правильно называть их *модули множественного доступа* (*MultistationAccess Unit — MAU*, или *MSAU*). Компания IBM называет MAU, который может контролироваться с удаленного узла, контролируемым модулем доступа *(Controlled Access Unit — CAU).* Причина, по которой эти устройства не принадлежат концентраторам (и по которой они значительно дороже большинства концентраторов), является следствием способности этих устройств реконфигурировать себя на ходу, по мере того, как узлы вводятся и выводятся из системы. Это более сложная задача, чем простое слежение за работоспособностью соединения, и для ее выполнения требуется более дорогая аппаратура.

С математической точки зрения технология Token Ring ведет себя беспристрастно по отношению ко всем участникам и гарантирует, что сеть не будет захлестнута трафиком. Технологию Token Ring можно назвать *беспристрастной,* поскольку она постоянно передает право пересылки сообщений от одного узла сети другому. Это осуществляется в виде специального сообщения, называемого *маркером (token).* Чтобы отправить сообщение, компьютер должен ждать до тех пор, пока не завладеет маркером. Маркер не освобождается до тех пор, пока сообщение не будет доставлено (или пока не станет очевидным, что оно не может быть доставлено). Всем предоставляются равные возможности использования маркера.

Мы предлагаем вам самый простой способ представить себе, как работает технология Token Ring. Чтобы отправить сообщение, ваша система ожидает маркер. Когда маркер приходит, если он уже не несет сообщения, ваша система прикрепляет ваше сообщение к маркеру и затем отправляет маркер (и сообщение) предполагаемому получателю. Получив адресованный ему маркер, получатель копирует прикрепленное сообщение и передает маркер по кольцу. Когда маркер возвращается в вашу систему, она забирает ваше сообщение и отправляет маркер (без сообщения) следующему компьютеру по направлению трафика кольца.

Сильные и слабые стороны Token Ring

К сильным сторонам Token Ring относятся равный доступ ко всем устройствам и гарантированная доставка сообщений. Сеть Token Ring работает надежно и предсказуемо, даже когда загружена на всю мощность. Сети Token Ring обеспечивают две скорости: 4 и 16 Мбит/с. Более старая медленная версия работает на скорости 4 Мбит/с. Это составляет 40% от теоретической пропускной способности для 10-мегабитовой Ethernet, но лишь немногим меньше базовой эффективной скорости Ethernet.

Новейшая высокоскоростная версия Token Ring функционирует со скоростью 16 Мбит/с, или 160% от базовой скорости Ethernet. Она может обрабатывать в три-четыре раза больше данных, поскольку допускает одновременное использование нескольких маркеров при 100-процентном использовании пропускной способности. Ждет своего часа полнодуплексная реализация технологии Token Ring, которая работает во многом аналогично Ethernet. Что касается более высоких скоростей, в стадии конструирования находится 100-мегабитовая версия Token Ring.

Мы поняли вашу мысль: "Если технология Token Ring так хороша, зачем покупать Ethernet?" Технология Token Ring обладает недостатками, которые в меньшей степени связаны с техническими аспектами и в большей — с негибкостью и стоимостью. Основным недостатком Token Ring является требование к наличию дорогостоящих устройств MAU, о которых мы говорили в предыдущем разделе. Также Token Ring требует прокладки двух жил кабеля от каждого компьютера к каждому порту концентратора. (Одна — для прохождения исходящих сигналов, вторая — для прохождения обратных сигналов.) Эти требования повышают стоимость Token Ring и уменьшают максимально допустимое расстояние между компьютерами и концентраторами. Кроме того, технология Token Ring отличается большей сложностью и требует более качественных коннекторов, чем Ethernet.

Token Ring во всем разнообразии

Существуют реализации Token Ring для таких сред, как витая пара и волоконно-оптические кабели; при этом витая пара, без сомнения, остается самой широко распространенной реализацией и представляет собой наиболее привлекательную среду для подключения настольных систем к концентраторам. Волоконно-оптический кабель представляет собой альтернативу для покрытия больших расстояний и организации гирляндной цепи на основе устройств MAU. В сетях Token Ring нечасто используются кабели типа *экранированной витой пары (shielded twisted pair — STP)*. Из-за ограничений на длину отдельного кабеля и ограничений на максимальные размеры кольца прокладка кабелей для сети Token Ring требует более тщательного планирования и "жонглирования" цифрами, чем укладка кабеля для сетей Ethernet.

Коммерческая сторона Token Ring

С точки зрения выигрыша в затратах преимущества Token Ring по надежности, равноправию узлов и гарантированной производительности недостаточны, чтобы платить за нее большую цену. Сегодня Token Ring обойдется вам в лучшем случае на 75, а в худшем — на 150% дороже, чем Ethernet, без обязательного обеспечения значительных преимуществ в производительности или надежности. Хотя существуют две противоположные точки зрения

на этот вопрос ("Забудьте Token Ring. Ethernet здесь правит бал" и "Мы сторонники доступа с передачей маркера. Что такое Ethernet?"), мы не станем категорически поддерживать ни одну из них. Если кто-то предлагает вам сеть Token Ring по цене, которая слишком хороша, чтобы пройти мимо, или если ее применение вызвано внешними обстоятельствами, — тогда используйте ее. Технология Token Ring работает просто отлично. Однако из-за высокой стоимости и сложности мы не рекомендуем ее как технологию, подходящую для того, чтобы начать создание сети.

Другие сетевые технологии

Если, приступая к чтению этого раздела, вы с любопытством думаете: "Что же там еще?", то вас может удивить отсутствие в этой книге вашей любимой сетевой технологии. Мы чувствуем себя неловко из-за необходимости говорить нелицеприятные вещи, но если вы не используете Ethernet или Token Ring, вам, возможно, придется много натерпеться от вашей сети (или вы, во всяком случае, выбрали не самый легкий путь создания сети). Уж извините!

В действительности сегодня используются сотни других типов сетевых технологий. Одна такая технология найдется, по меньшей мере, для каждой буквы алфавита от A (для ARCnet) до X (для xDSL). Если вам кажется, что от такого изобилия аббревиатур голова может пойти кругом, вы не одиноки. Распространение экзотических технологий может также быть проблемой и для Windows Server 2003. Мудрый совет: если вы используете экзотическую сетевую технологию, прежде чем потратить деньги на ПО, убедитесь в том, что Windows Server 2003 работает с ней.

Хорошая новость заключается в том, что Windows 2003 работает с разумным подмножеством технологий. Плохая новость заключается в том, что вам необходимо провести некоторое исследование, чтобы определить, входит ли технология, с которой вы работаете, в число технологий, поддерживаемых Windows 2003. Но еще худшая новость заключается в том, что вам придется немало потрудиться, чтобы сделать элементарные веши, которые менее экзотические технологии выполняют запросто, и, кроме того, вам, возможно, также придется отказаться от некоторых развитых возможностей, таких как подключенные к сети принтеры и другие периферийные устройства.

Однако работа с технологиями, отличными от Ethernet и Token Ring, не обязательно приводит к таким печальным последствиям. В следующих двух разделах мы выполним за вас домашнее задание и рассмотрим парочку потенциально полезных сетевых технологий, которые встречаются среди довольно большого подмножества сетей масштаба предприятия и поддерживаются Windows 2003.

Подключитесь к магистрали

Одна из сетевых технологий, своего рода "рабочая лошадка", которую можно встретить во многих сетях, в особенности масштаба кампуса, называется технологией *FDDI (Fiber Distributed Data Interface— распределенный интерфейс передачи данных по волоконно-оптическим каналам)*. Технология FDDI использует метод доступа с передачей маркера. Кабельная система сетей FDDI образует подлинную кольцевую топологию, но состоит из двух колец. Одно из колец передает сообщения по часовой стрелке, другое — против часовой стрелки. Если какое-либо из колец отказывает, второе автоматически берет обслуживание на себя как резервное. Но что еще лучше, если оба кольца порвутся в одном месте (ох уж эти ребята на экскаваторе из вашего кампуса!), два кольца автоматически стыкуются, образуя кольцо, которое в два раза длиннее исходного кольца и по-прежнему способно работать.

Наибольшее преимущество, которым отличается технология FDDI,— скорость 100 Мбит/с, — сегодня не такое уж "большое дело". FDDI поддерживает сети длиной до 100 км в окружности. FDDI может поддерживать до 500 активных устройств на одно кольцо,

что превышает количество устройств, поддерживаемых технологиями, которые мы подробно рассмотрели в этой главе.

Отрицательной стороной FDDI является необходимость использования волоконно-оптических кабелей при передаче данных на любые расстояния. Существует аналогичная технология передачи данных по медным проводам — CDDI (где *C* означает copper — медь), но она не поддерживает кабели длиной более 230 м, поэтому она непрактична, кроме как в случаях соединения рабочих станций.

Еще одно негативное свойство FDDI — стоимость. Приобретение и установка волоконно-оптических кабелей обходится дороже других типов кабелей, а сетевая карта для FDDI стоит от 700 до 1800 долларов. Технология FDDI лучше всего подходит для центрального канала сети кампуса (говоря технически языком — *магистрали* (*backbone*)), если в качестве альтернативы (или по требованию) не выбирается технология Gigabit Ethernet.

Разгоняемся до ATM

Восходящая звезда на небосклоне высокоскоростных сетей — технология *ATM (Asynchronous Transfer Mode — асинхронный режим передачи)*. В последние годы несколько компаний вывели на рынок оборудование для ЛС, ориентированное на использование ATM. Междугородные телефонные компании уже используют версии ATM, которые работают со скоростями 155 и 662 Мбит/с, а современные спецификации ATM также поддерживают скорости 1,2 и 2,4 Гбит/с. ATM — технология быстрой коммугации, которая требует коммутирующих устройств наподобие концентраторов и наличия сетевого интерфейса у каждого из компьютеров. Чтобы внедрить технологию ATM на своих компьютерах, вам необходимо затратить по меньшей мере 2000 долларов на рабочую станцию (включая ассигнования на коммутатор и волоконно-оптический кабель). Это, возможно, объясняет, почему ATM намного более популярна как технология сетевых магистралей, чем средство для подключения компьютеров к сети.

На рис. 4.3 показана сравнительная диаграмма скоростей различных сетевых технологий (которая вам кое-что пояснит), однако лучший способ понять, что к чему, — воспользоваться Internet и обратиться к "коллективному разуму", который всегда наготове. Вы можете подписаться на любую из телеконференций Usenet Windows компании Microsoft, посвященных Windows 2003, посредством Web-узла news://msnews.microsoft.com;воспользоваться собственной интерактивной службой Microsoft, Microsoft Network (MSN), обратившись на Web-узел www.msn.com; или присоединиться к одному из многочисленных списков рассылки, посвященных Windows 2003, и спросить: "Работает ли моя сетевая технология (здесь вставьте название вашей сетевой технологии) с Windows Server 2003?" Если у вас нет доступа к интерактивным информационным ресурсам, спросите коллег и друзей. Думаем, при таком количестве пользователей во всем мире вам не придется слишком долго искать того, кто сможет вам помочь.

Вспомогательное оборудование

Иногда, чтобы создать сеть, помимо компьютеров, вам могут потребоваться многочисленные устройства — в особенности, когда сеть перерастает рамки простой группы пользователей. Не останавливаясь слишком подробно на возможностях и более сложных функциях, мы приводим перечень устройств, пригодных для большинства сетевых технологий (или включающих интерфейс, основанный на таких технологиях), которые вы можете использовать для расширения или соединения существующих сетей.

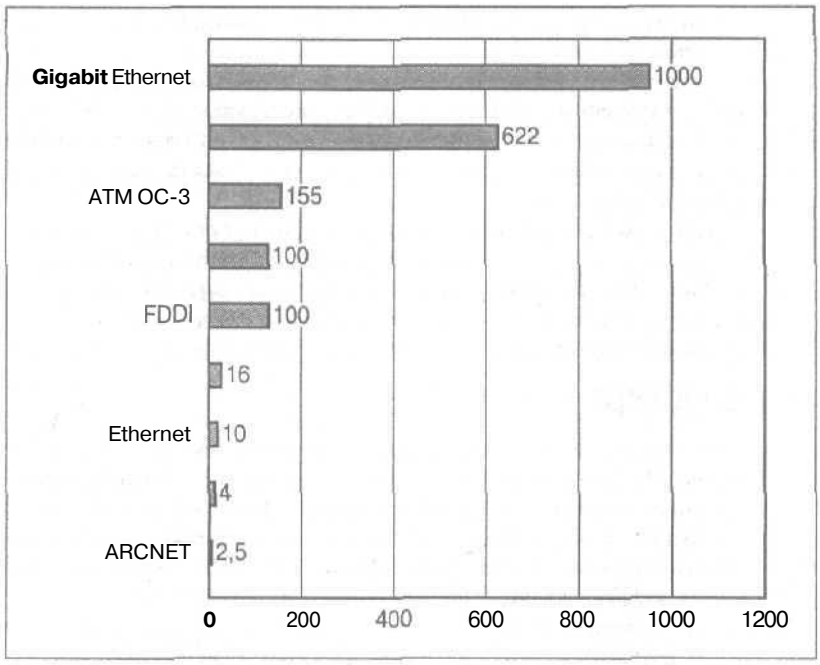


Рис. 4.3. Порядок скоростей передачи данных, обеспечиваемых сетевыми технологиями

- ✓ **Повторитель** (repeater). *Повторитель* (или *репитер)* — простое сетевое устройство, которое считывает входящие сигналы из одного соединения и затем отправляет их одному или нескольким другим соединениям (называемым *портами*). В названии устройства заключена простая идея его работы: оно "повторяет" в точности то (без исключения), что оно "слышит". Повторители могут связывать только те сегменты среды, которые используют одну и ту же сетевую технологию, однако эти сегменты могут принадлежать разным типам сетевых сред. Повторители работают на физическом уровне модели OSI. (Модель OSI рассматривалась в главе 3.)

Используйте повторители в тех случаях, когда вы достигли допустимых пределов длины кабеля, которую поддерживает сетевая технология. Повторители позволяют вам расширить сеть за пределы, которые она иначе не может перейти. Заметьте, что сетевая технология также подчиняется правилам, которые регулируют максимальное количество повторителей, находящихся между любым отправителем и любым получателем в сети.

- ✓ Мост (bridge). *Мост* — это сетевое устройство, которое проверяет адреса входящего сетевого трафика и переносит входящие сообщения в другие сетевые сегменты только в том случае, если они могут достичь своего адресата через эти сегменты (или прямо по ним). В названии устройства заключается идея его функционирования: оно работает до некоторой степени как интеллектуальный канал между сетями и проверяет низкоуровневые адреса оборудования, чтобы решить, что можно пропустить из одной сети в другую. Мосты работают на уровне канала передачи данных (более точно, на подуровне управления доступом к среде — MAC) модели OSI.

Мосты могут не только связывать сегменты среды в рамках одной и той же сетевой технологии, так называемые транслирующие мосты могут соединять сетевые сегменты, которые используют различные сетевые технологии (распространенный пример — соединение сетей FDDI и Ethernet). Однако протоколы по обе стороны устройства должны оставаться одинаковыми.

Используйте мосты в тех случаях, когда ваша сеть включает протоколы без маршрутизации, такие как протокол NetBEUI или DLC (Data Link Control — протокол управления каналом передачи данных), и когда подобный трафик должен пересылаться из одного сетевого сегмента в другой. Заметьте, что некоторые маршрутизаторы включают функции запараллеливания (установления мостов) и что гибридные устройства, называемые мостами-маршрутизаторами, могут выполнять функции запараллеливания и маршрутизации.

- Маршрутизаторы (router). *Маршрутизатор* — сложное сетевое устройство, которое читает и разрешает сетевые адреса из входящего трафика в сетевые имена. Маршрутизаторы выполняют все виды операций над такими данными, включая фильтрацию входящих данных по адресу, манипулирование несколькими протоколами, блокирование или санкционирование определенных типов протоколов, а также определенных диапазонов адресов, связанных с определенными протоколами, и многие другие. Маршрутизаторы работают на сетевом уровне модели OSI. (Подробности см. в главе 3.)

  Маршрутизаторы могут соединять сети, использующие различные технологии, и могут даже изменять формат данных для передачи выходному порту, технология которого отличается от технологии, поддерживаемой входным портом. В качестве наиболее типичного примера здесь можно привести соединение сети Token Ring, работающей со скоростью 16 Мбит/с, и сети Ethernet. Поскольку технология Token Ring поддерживает блоки сообщений намного большего объема, чем Ethernet, маршрутизатор может быть вынужден делить одно сообщение Token Ring на — ни много ни мало — 44 эквивалентных сообщения Ethernet.

  Маршрутизаторы — это устройства, которые делают возможным независимое функционирование двух сетей, заставляя их в случае необходимости обмениваться информацией. Маршрутизаторам обязаны своим существованием такие феномены, как Internet, в росте которых им принадлежит определяющая роль. Используйте маршрутизаторы, когда вы стремитесь эксплуатировать и контролировать вашу сеть (или сети) и в то же время иметь возможность соединения ее с другими сетями.

- Мост-маршрутизатор (bridge router, brouter). *Мост-маршрутизатор* сочетает в себе функции моста и маршрутизатора, т.е. он работает подобно мосту для протоколов без маршрутизации и подобно маршрутизатору для протоколов с маршрутизацией. Мосты-маршрутизаторы, как правило, применяются в сетях, использующих оба типа протоколов. Они также используются в тех случаях, когда для локальной сети необходимы протоколы с запараллеливанием или маршрутизацией, но доступ к Internet или другим общедоступным сетям требует маршрутизации протоколов с маршрутизацией. Мосты-маршрутизаторы работают как на канальном, так и на сетевом уровне модели OSI.
- Шлюз (gateway). *Шлюз* — это устройство, которое преобразует информацию прикладного уровня из одного типа среды в другой тип среды. Типичным примером шлюза является шлюз электронной почты, который преобразует

формат Microsoft Exchange в собственный почтовый формат Internet, известный как *SMTP (Simple Mail Transfer Protocol — упрощенный протокол электронной почты)*, и наоборот.

Другие шлюзы могут осуществлять преобразование между различными комплектами протоколов, такими как протоколы SNA и TCP/IP. Кроме того, существуют шлюзы, которые поддерживают перемещение данных между другими разнородными приложениями одного типа, такими как системы управления базами данных или системы обработки транзакций. Шлюзы функционируют в основном на верхних уровнях модели OSI (см. главу 3) и сосредоточены на сеансовом и прикладном уровнях и на уровне представления данных.

По мере того как вы преодолевали эту "гору" из вспомогательных устройств (начиная от "приземленных" повторителей и восходя к шлюзам), их сложность и возможности возрастали, а их скорость и общая производительность падали. Это является следствием того, что каждый шаг вверх по этой "горе" связан со все большими возможностями по обработке данных, которые требуют процессорного времени и изощренного программирования и поэтому приводят к общему снижению производительности устройств.

Вы часто могли видеть устройства, такие как повторители и мосты, которые выглядят как простые черные коробочки, которые более-менее готовы, чтобы их подключить и использовать. С другой стороны, маршрутизаторы и мосты-маршрутизаторы представляют собой специализированные, мощные и высокоскоростные компьютеры, в которые вставляются две или больше интерфейсных плат (по одной на каждое соединение, которое вы устанавливаете с этим устройством).

Система Windows 2003 включает мощные встроенные возможности маршрутизации, такие как сервер *RRAS (Routing and Remote Access Server — сервер маршрутизации и удаленного доступа)*. Кроме того, для усовершенствования возможностей системы Windows Server 2003 в нее можно добавить дополнительное ПО наподобие сервера *ISA (Internet Security and Administration Server — сервер безопасности и администрирования Internet)*. С другой стороны, под шлюзы, как правило, отводят универсальный компьютер, но он также обычно предназначен для выполнения только этой работы.

Комбинирование и сочетание сетевых технологий

Сетевые технологии могут легко комбинироваться и сочетаться в рамках единой сетевой технологии, но комплексирование сетевых технологий требует более сложного оборудования.

- **Комплексирование различных сред в рамках** определенной **сетевой технологии.** Большинство поставщиков предлагают простые устройства (повторители и мосты) для комплексирования сетевых сегментов, которые используют разные типы сред, такие как витая пара (lOBaseT) и коаксиальный кабель (10Base2) для Ethernet. Windows Server 2003 может работать с несколькими сетевыми интерфейсами, каждый из которых предназначен для работы со своим типом среды.
- **Комплексирование различных сетевых технологий в рамках сети.** До тех пор, пока типы протоколов совпадают, маршрутизаторы или мосты-маршрутизаторы могут справиться с задачей, например, такой, как комплексирование сегментов Token Ring и Ethernet. Аналогично, встроенные возможности маршрутизации системы Windows Server 2003 позволяют ей легко работать в качестве маршрутизатора для

комплексирования различных сетевых технологий. Она просто не может выполнять эту функцию так же быстро, как это делает специализированный высококлассный маршрутизатор наподобие устройства Nortel Networks от Cisco Systems.

- ✓ **Комплексирование принципиально различных протоколов или приложений.** Когда принципиально различные протоколы или приложения должны обмениваться данными, наступает час шлюзов. Этот обмен связан со значительно большими затратами и интеллектуальными возможностями, чем в состоянии обеспечить низкоуровневые службы мостов и маршрутизаторов. Однако шлюзы должны также учитывать значительно больше нюансов и функциональных возможностей, чем другие устройства. Это, возможно, объясняет, почему они чаще являются источником проблем, чем другие альтернативы.

Диалоговое окно настройки протокола TCP/IP для Windows Server 2003 содержит вопросы, касающиеся адреса шлюза. В этом конкретном случае Windows Server 2003 использует термин *шлюз* в смысле, отличном от рассматривавшегося здесь. При настройке конфигурации протокола TCP/IP Windows Server 2003 рассматривает термин шлюз как синоним термина маршрутизатор и в действительности указывает на устройство, которое может переправлять пакеты не прямо в локальный кабельный сегмент для доставки во внешние системы. Будьте внимательны и учитывайте это обстоятельство при настройке конфигурации протокола TCP/IP для Windows Server 2003!

Часть II

Подключение оборудования

"Я полагаю, вы могли бы считать это концентратором нашей сети".

В этой части...

В части Г мы описали основные сетевые термины и понятия, а в части II попытаемся заняться более осязаемыми вещами — оборудованием и проводкой, — которые необходимы для надлежащей работы каждой сети.

Стараясь превратить сетевые концепции в работающую сеть, вы изучите базовые принципы планировки и проектирования сети. После этого вы приметесь за входы и выходы плат сетевого интерфейса, или, как его часто называют профессионалы, — сетевых адаптеров. После установки плат на место наступит очередь подключения к ним кабелей.

• По ходу дела вы сможете уяснить, как создать новую сеть или расширить старую и как критически оценить существующую сеть. Вы также поймете, как соединить части сети, чтобы создать гармоничное целое, а не набор из железного хлама. Ваша цель — понять, что представляют собой все компоненты сети и как заставить их действовать слаженно.

Глава 5

Основы проектирования сети

В этой главе...

- Проектирование работоспособной сети
- Знакомство с основами проектирования сетей
- Расположение серверов и других сетевых устройств
- Двойная проверка вашего проекта
- Организация сети по логическим принципам
- Составление схемы сети

Независимо от того, создаете ли вы новую или обновляете существующую сеть, основной подход остается неизменным. Сначала вы продумываете, что вы желаете реализовать, а затем собираете компоненты, необходимые для воплощения ваших замыслов. После этого вы должны осуществить свои планы в соответствии с составленным проектом. Выполнение любого успешного плана связано с соединением всех необходимых компонентов, применением четких организационных принципов к вашей сети и отражением в документации всего того, что добавляется к сети (или уже находится там на своем месте).

Начнем с начала

Когда вы составляете сетевой проект, начинайте с анализа ваших требований. Если вы создаете сеть с нуля, этот этап может занять недели или месяцы работы; если вы просто расширяете или восстанавливаете существующую сеть, планирование может занять у вас один день или и того меньше.

Каковы бы ни были рамки проекта, содержание вашего плана должно выглядеть следующим образом.

- ✓ **Краткая формулировка общих целей и расширенная формулировка требований с учетом следующих вопросов: к каким приложениям и службам необходим доступ пользователям; оценки требований к пропускной способности канала "пользователи–сервер" и канала "сервер–сервер" (по необходимости).**

  Пример. Новая сеть корпорации XYZ должна обеспечивать 60 пользователям доступ к службам файлов и печати, а также доступ к базам данных сбыта и запасов, работающим под управлением MS SQL Server. Каждому пользователю потребуется канал с пропускной способностью не более 1 Мбит/с, кроме того, в рабочее время требования к пропускной способности канала "сервер–сервер" отсутствуют, поскольку все резервное копирование планируется выполнять в нерабочее время и в выходные дни.

- ✓ **Полный перечень всех элементов, которые вы должны приобрести, чтобы удовлетворить этим целям.**

  Пример. Три различных сервера отделов (бухгалтерии, производственного и сбытового) должны работать в качестве маршрутизаторов, связывая два сетевых сегмента по 10 пользователей в каждом из общего количества в 6 пользовательских сегментов, созданных на базе 10-мегабитовой сети Ethernet. Три сервера должны соединяться магистралью, которая образована 100-мегабитовой сетью Ethernet, использующей спецификацию 100BaseT. Мы должны купить шесть 16-портовых концентраторов для Ethernet 10/100 Мбит/с (по одному на пользовательский сегмент), чтобы оставить место для наращивания сети, а также три двухпроцессорные серверные машины Intel Zeon с процессорами Pentium II частотой 500 МГц, оснащенные 512 Мбайт ОП и дисковой памятью объемом 24 Гбайт. Сервер бухгалтерии должен быть оснащен ленточным DLT-устройством объемом 80 Гбайт, подключенным таким образом, чтобы иметь возможность резервного копирования данных всех трех серверов по магистрали. (DLT — digital linear tape (лента для цифровой записи с последовательным доступом).)

- ✓ **Описание роли каждого элемента, которую он играет в сети, местоположение каждого элемента в сети, конфигурация каждого элемента и время, за которое вы планируете добавить каждый элемент в процессе установки сети.**

  Вы должны использовать схему или набор планов, которые помогут вам разместить кабели, компьютеры и другие компоненты, а также временной график, чтобы указать порядок, в котором они должны быть установлены.

  Пример. Сервер бухгалтерии должен обслуживать пользователей из бухгалтерии и производственного отдела; сервер производственного отдела должен обслуживать пользователей из производственного и конструкторского отделов; сервер отдела сбыта должен обслуживать пользователей из администрации, а также из отделов сбыта и маркетинга. Все серверы, магистраль и все концентраторы должны быть установлены, когда компания будет закрыта между Рождеством и Новым годом. Сеть должна быть введена в эксплуатацию после возобновления повседневной деятельности компании. Схема этой сети показана на рис. 5.1.

- ✓ **План испытаний, который описывает, как вы планируете испытывать отдельные элементы, отдельные сегменты кабеля, а также сеть в целом, чтобы убедиться, что после установки все функционирует должным образом.**

  Пример. Три сервера должны быть установлены первыми и испытаны по отдельности в течение выходных накануне Рождественских каникул. 100-мегабитовая магистраль должна быть установлена 23 или 24 декабря. 28 декабря магистраль должна быть испытана. 28 или 29 декабря должны быть установлены и испытаны концентраторы. 30 декабря рабочие станции на всех 10-мегабитовых кабельных сегментах должны быть подключены к новым концентраторам для Ethernet 10/100 Мбит/с и испытаны по отдельности. С 31 декабря по 2 января сеть в целом должна быть испытана с помощью автоматизированного тестового ПО. 3 января специалист по сетям должен посетить нашу площадку с Бобом, администратором узла, чтобы внести последние изменения, исправления и выполнить настройки. Мы полагаем, что сеть будет готова к использованию 4 января.

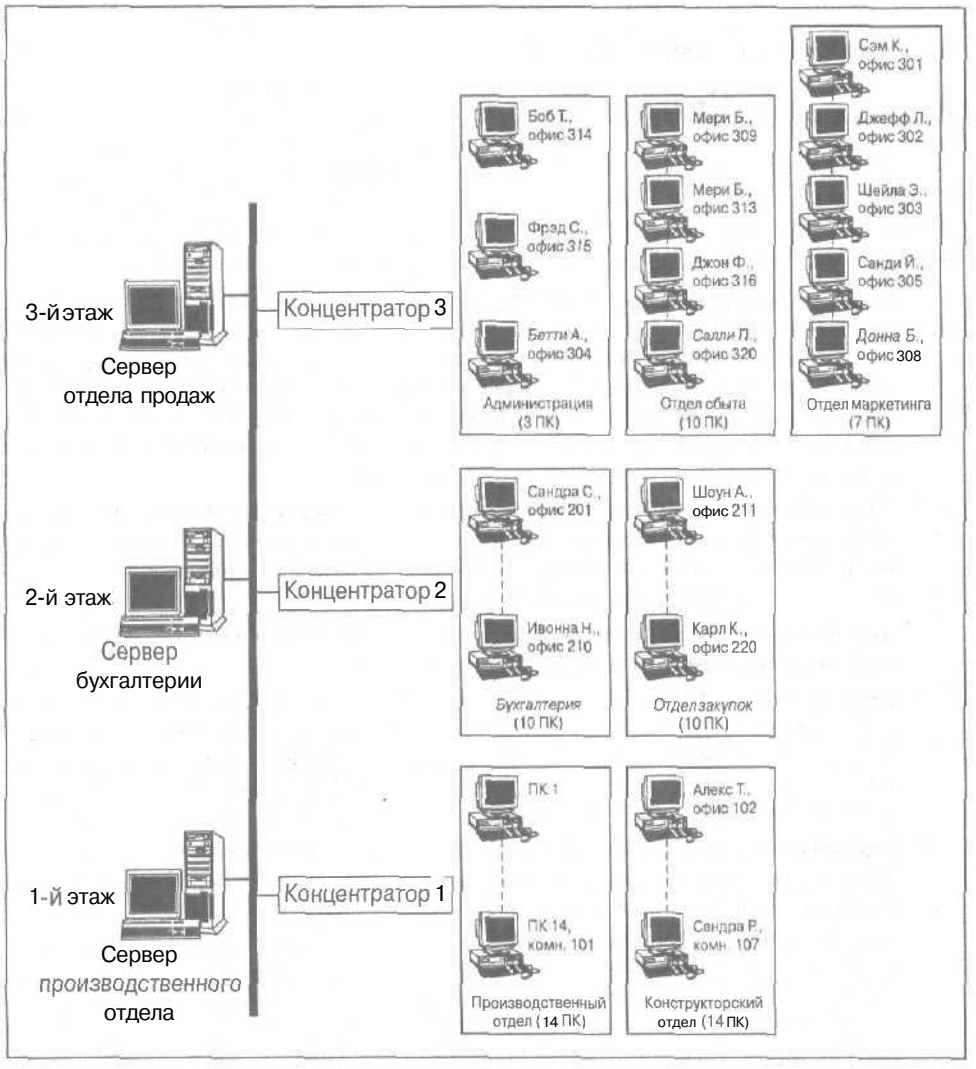


Рис. 5.1. Простая схема сети компании XYZ

План помогает решить, куда вы должны поместить ключевые элементы сети, такие как серверы, концентраторы и др. Что более важно, план также помогает вам определить, какой тип сетевой технологии и какая пропускная способность вам требуются для того, чтобы достичь поставленных целей. Поскольку большинство предприятий работает в соответствии с бюджетом, план также поможет вам удостовериться в том, что вы не выходите за рамки выделенных средств и не пытаетесь внедрить более экзотическую технологию, чем в состоянии себе позволить.

Ваш план реализации сети также должен помочь оценить существующую магистраль вашей сети и, возможно, запланировать ее модификацию, чтобы обеспечить передачу всего трафика, который обычно концентрируется в таких ответственных сетевых сегментах. (Вопросы, связанные с пропускной способностью, более подробно мы обсудим в главе 7.)

Элементарные основы проектирования сети

Количество возможных вариантов реализации, из которых вы можете выбирать при проектировании сети, бессчетно. Чтобы помочь вам провести различия между невозможными, возможными, приемлемыми и рекомендуемыми альтернативами проектных решений, мы предлагаем набор полезных руководящий принципов.

- ✓ Выберите сетевую технологию. При подключении новых устройств или наращивании существующей сети это нетрудное решение — оно просто требует выбора чего-то похожего или совместимого с тем, что вы уже используете. Что касается новых сетей, вам необходимо проанализировать, какого рода приложения и службы требуются пользователям. Для обычной офисной работы (электронная почта, обработка текстов, электронные таблицы, базовый доступ к базам данных и т.д.) вполне достаточно сети стандарта Ethernet 10 Мбит/с. Для приложений реального времени, а также приложений, генерирующих большой трафик, например, связанных с автоматизированным проектированием (computer-aided design — CAD), проведением видеоконференций, передачей по сети изображений и звука, больший смысл имеют настольные системы, работающие по стандарту Ethernet 100 Мбит/с.
- ✓ **Держитесь ближе к ресурсам.** При проектировании сети наиболее целесообразно минимизировать расстояние между пользователями и ресурсами, к которым они обращаются наиболее часто. Это относится к принтерам (чтобы доступ пользователей к выводным устройствам был максимально облегчен), серверам (чтобы длина кабелей не была слишком большой) и другим службам (таким как факсимильные аппараты, сканеры и копировальные устройства), к которым пользователям требуется непосредственный доступ для выполнения своей работы.
- ✓ **Создайте интерактивную рабочую среду.** При проектировании сети вам также необходимо учитывать принятый в вашем офисе стиль и порядок выполнения работы. (Например, если бухгалтерия и отдел закупок постоянно работают вместе, возможно, они должны совместно использовать сервер.) Это также применимо к типу сети, которую вы создаете. Для небольших компаний централизованный контроль и жесткая система безопасности могут стеснять работников; в больших компаниях централизованный контроль и строгая система безопасности являются нормой. Вы должны обслуживать коллективы, которые сложились в вашей организации, и использовать сеть, чтобы помогать пользователям обмениваться информацией и добиваться максимальной продуктивности труда.
- ✓ **Разместите серверы, концентраторы и другие важнейшие ресурсы.** Иногда места, где сосредоточена проводка — монтажные блоки, коммутационные центры и аппаратные (или кроссовые шкафы), — диктуют расположение определенного оборудования. Вы должны следить за расстоянием между этими местами и участками, где располагаются работники. В большинстве случаев офисы спроектированы таким образом, что обеспечивают прокладку кабелей от расположенных в центре коммутационных или аппаратных центров к группам офисных помещений. Если ваше рабочее пространство не позволяет этого, вам может потребоваться добавить новые аппаратные и коммутационные центры или переместить работников ближе к существующему оборудованию. Любое из этих решений требует времени и затрат значительных средств, поэтому позаботьтесь о том, чтобы привлечь руководство к выбору наиболее разумного варианта и планированию мер, которые помогут вашей организации справиться с подобными переменами.

- ✓ **Создайте подходящую магистраль данных.** В зависимости от выбранной технологии вам, вероятно, может потребоваться привести в порядок вашу сеть, чтобы включить в нее магистраль для данных, которые могли бы перемещаться по всей сети после соединения нескольких кабелей. Такой "тракт" может появиться между серверами, как в примере для корпорации XYZ, приведенном в начале главы. Подобная часть сети называется *магистралью данных,* или *магистралью (backbone).*

  Магистраль может быть чем-то простым, наподобие так называемой *вырожденной опорной сети (collapsed backbone),* в которой высокоскоростной коммутатор соединяет кабельные сегменты и обеспечивает единое высокоскоростное соединение между *всеми* кабельными сегментами. Магистраль может быть и чем-то сложным, наподобие *ступенчатой магистрали (staged backbone),* в которой промежуточные сегменты перескакивают с обычной 10-мегабитовой Ethernet на коммутируемую Ethernet или 100-мегабитовую Ethernet на сервере (как в примере для корпорации XYZ, упомянутом в начале этой главы). Более сложные магистрали могут даже включать сегмент Gigabit Ethernet для самых глубоких сегментов, которые отличаются наиболее высоким трафиком.

- ✓ **Запланируйте возможности для роста сети.** При планировании сети заложите в проект запас по меньшей мере в 30% неиспользуемых возможностей. Этот запас возможностей должен включать сетевые порты (неиспользуемые порты концентраторов), неиспользуемые сетевые кабели в офисах и кабелепроводах, а также запас пропускной способности отдельных сетевых сегментов. Таким образом, вы сможете обеспечить рост в пределах существующей среды в течение некоторого времени без постоянной переделки сети. Если скорость вашего годового роста превышает 30%, заложите в проект по меньшей мере этот годовой планируемый рост, а еще лучше — этот годовой планируемый рост *плюс* 30%.

- ✓ **Проводите работу внутри системы.** Создание сети в любой организации имеет не только техническую, но и политическую сторону. При планировании сети вы должны проводить работу внутри организации по меньшей мере в двух направлениях. Во-первых, позаботьтесь о том, чтобы руководство знало о ваших планах и одобряло их. Во-вторых, позаботьтесь о том, чтобы ваша деятельность по выполнению работ, контрактов, закупок и т.д. укладывалась в рамки правил и инструкций, принятых в вашей организации. Если пренебречь каким-либо из этих руководящих принципов, единственное, чего вы добьетесь, — это проблемы с сетью!

- ✓ **Проверяйте ваш проект.** После того как вы перенесете проект на бумагу, проанализируйте его с точки зрения ваших знаний о тех технологиях, которые в нем применяются. Особенно внимательно проверьте, удовлетворяют ли ограничениям, принятым для технологии, которую вы планируете использовать, такие параметры, как максимальная длина кабелей, максимальное количество устройств на сегмент и максимальное количество кабельных сегментов и устройств между любыми двумя концами сети. Вам совсем не требуется создавать сеть, которая выходит за рамки этих ограничений. Если это произойдет, ваша сеть, возможно, не будет работать или, что еще хуже, будет работать какое-то время, а затем прекратит работу, когда вы добавите к ней новых пользователей или устройства. Если вы проверите все это заблаговременно, вам не нужно будет стараться создавать нечто, что не работает или в своей основе таит проблемы.

- ✓ **Организуйте "санитарную проверку".** После того как вы перенесете проект на бумагу и проверите свою работу, вы должны спросить совета у одного или нескольких экспертов по сетям. Переработка проекта сети всегда легче, если он все еще остается на

бумаге, поскольку вам не придется исправлять ошибочный проект после того, как вы создадите сеть. Чем более квалифицированный совет вы получите до начала создания сети, тем более состоятельными будут принимаемые вами решения в долговременной перспективе. В действительности этот совет стоит того, чтобы за него заплатить, поскольку он сохранит ваше душевное спокойствие (или вашу работу, если на то пошло).

Хотя этот перечень принципов проектирования сети не является исчерпывающим, он поможет вам в проектировании сети, которая вполне удовлетворит вашу организацию. Поскольку эти принципы учитывают наряду с технологическими такие организационные аспекты, как принятый в организации стиль работы, внутрифирменная политика, нормы и правила поведения, созданная сеть должна хорошо послужить вашей организации не только из технических соображений.

Устанавливаем сетевые устройства

После того как план составлен, вы должны купить необходимое оборудование, кабели, коннекторы и пр. и приступить к развертыванию компонентов, которые заставляют сеть работать. Прежде чем приступить к размещению основного сетевого оборудования — включая серверы, концентраторы и маршрутизаторы, — вам необходимо принять некоторые важные решения о том, куда их поместить.

Для небольших организаций, насчитывающих не больше 25 сотрудников, не имеет смысла использовать отдельные закрытые помещения для хранения концентраторов и серверов. Небольшие организации отличаются более неформальным характером и менее склонны выделять отдельной строкой бюджета средства на содержание персонала поддержки информационной системы (ИС), работающего полный рабочий день. В этих условиях сетевую технику обычно помещают туда же, где находится вся остальная техника, — в открытые помещения вместе со всем остальным оборудованием, что обеспечивает легкий доступ к ней всем и каждому. Если вы поместили сетевую технику в общедоступном месте, позаботьтесь о том, чтобы подсоединяться к подобному оборудованию могли только пользователи, обладающие надлежащим паролем. В противном случае настоятельно рекомендуется поместить ее под замок.

Более крупные организации в большей мере заботятся о безопасности и контроле и поэтому обычно помещают основные сетевые компоненты в запертых аппаратных и монтажных шкафах или центрах коммутации в различных местах по всем их офисам. Поскольку оборудование должно находиться вблизи проводки, нет ничего необычного в том, что серверы размещаются в монтажных шкафах вместе с монтажными кабелями, концентраторами и другим сетевым оборудованием.

В эти помещения разрешен доступ только уполномоченному персоналу. Аналогично, только уполномоченному персоналу должно быть разрешено добавлять пользователей или оборудование к сети, обычно в рамках системы регулярно планируемых процедур обновления или сопровождения. Это означает, например, размещение в офисных зданиях одного-двух монтажных шкафов или аппаратных на каждом этаже, где только уполномоченный персонал обладает ключами или кодами доступа для проникновения в эти помещения,

Выберите подход к размещению ваших серверов, который имеет смысл для вашей организации, и придерживайтесь его. Если вы следуете определенным правилам размещения оборудования, расскажите о них сотрудникам, чтобы они понимали, что происходит. В действительности формулирование политики безопасности для большинства сетей — это ход, и вы должны регулярно подробно объяснять эту политику сотрудникам. (Подробная информация об этой теме содержится в главе 18.)

Большинство небольших и средних компаний, таких как воображаемая корпорация XYZ, упомянутая в начале этой главы, размещают свои серверы в небольших, запертых комнатах в конце каждого этажа, которые они занимают в офисном здании. При этом расстояние между пользовательскими настольными системами и коммутационными центрами остается на приемлемо невысоком уровне и позволяет поместить серверы вдоль монтажных блоков и концентраторов, которые они используют, что помогает в управлении проводкой. Этот подход также обеспечивает контролируемый доступ к оборудованию и ПО, которые заставляют сеть работать, только из небольшого количества мест, находящихся под строгим контролем. Наконец, он отвечает потребности в подходящем вентилировании и управлении питанием, которые необходимы для надлежащей работы серверов и концентраторов и которые не обеспечивают многие типы монтажных шкафов.

Всегда проверяйте свою работу!

Обычно вы прокладываете кабель и устанавливаете оборудование одновременно с созданием сети. Вы можете проложить кабель для вашей сети, установить и настроить конфигурацию оборудования самостоятельно, можете заключить контракт на прокладку кабеля и установку оборудования со сторонним исполнителем либо выбрать некий промежуточной вариант выполнения работ. Какой бы способ вы ни выбрали, в некоторый момент вы будете готовы соединить завершенные фрагменты вашей сети.

Когда речь идет о прокладке кабеля, мы настоятельно рекомендуем нанять опытных монтажников кабельных систем с хорошей репутацией. Компания, которая владеет вашим офисным зданием и эксплуатирует его, может даже потребовать привлечь для выполнения подобной работы монтажников, имеющих специальную лицензию. Существует несколько причин, оправдывающих подобные требования.

- Строгое соблюдение строительных и противопожарных норм и правил является обязательным, а потому привлечение опытных профессионалов — хороший способ избежать проблем.
- ✓ Расположение и прокладка кабеля — дело тонкое; подготовленные профессионалы знают, как обойти потенциально слабые места, и всегда проверяют свою работу, чтобы убедиться, что сеть будет работать надлежащим образом.
- ✓ Высокоскоростные сети требуют намного более филигранной техники, поэтому в них чаще возникают проблемы, чем в низкоскоростных сетях. Чем быстрее вам необходимо запустить вашу сеть, тем с большей долей уверенности вам удастся этого достичь, если вы поручите кабельную систему специалистам.

Мы настоятельно рекомендуем вводить в действие сеть в виде небольших управляемых фрагментов. При установке нескольких кабельных сегментов вводите отдельные кабельные системы одну за другой и проводите их испытания, чтобы удостовериться в работоспособности каждой из них, прежде чем соединять их. Также, если вы устанавливаете магистраль или серверный кластер, проведите испытания всех компонентов по отдельности, прежде чем пытаться соединить их вместе.

При установке оборудования следуйте этим же принципам. После установки и настройки конфигурации машины проверьте ее сами, чтобы убедиться в ее работоспособности. Применение этих же правил уместно при установке концентраторов и маршрутизаторов, а также серверов и настольных компьютеров.

Наши советы о необходимости проверки компонентов и фрагментов сети и постепенном наращивании ее сложности исходят из опыта. Мы прошли этот тяжкий путь, когда попытки создать сеть сразу, наспех соединив все составляющие, приводят к проблемам, которые слишком трудно поддаются решению, поскольку связаны со слишком большим количеством неизвестных.

Не упускайте сеть из виду

После того как сеть создана, вы можете поддаться искушению отдохнуть, чтобы немного насладиться своим успехом. Как-никак вы заслужили его, правда? Конечно, хотя вы определенно заслуживаете одобрения, вы также должны понимать, что настоящая работа начинается сразу после того, как пользователи станут работать с сетью (или вновь введенным фрагментом существующей сети). Если вы отвечаете за сеть, то должны не только управлять ходом дел до момента ввода сети, но и продолжать следить за тем, чтобы она нормально функционировала в последующем.

Несмотря на то что созданная или расширенная сеть удовлетворяет первоначальным требованиям пользователей, способность любой сети удовлетворять дальнейшие потребности пользователей со временем уменьшается. Рост, технологические изменения и новые приложения и службы служат гарантией того, что ничто долго не стоит на месте, — это касается вашей сети, а также систем и служб, которые ваша сеть предоставляет в распоряжение пользователей.

Поэтому вам необходимо проводить регулярный анализ того, насколько хорошо ваша сеть удовлетворяет потребности пользователей. В небольших организациях и организациях, которые отличаются невысокими темпами роста, анализ можно проводить не чаще одного раза в год. В больших и быстро растущих организациях подобный анализ сети следует проводить ежеквартально.

Анализ сети должен включать по меньшей мере три момента.

- ✓ Анализ трафика и интенсивности использования сети. Подобный анализ вы можете проводить самостоятельно с использованием встроенных средств и возможностей Windows Server 2003 наподобие утилиты System Monitor (Системный монитор) и программных средств сторонних разработчиков. Идея заключается в том, чтобы получить "мгновенный снимок" вашей сети в условиях обычной, минимальной и пиковой нагрузки. Если какой-либо из этих типов нагрузки выходит за пределы, которые в достаточной степени поддерживаются текущим проектом сети, начинайте планировать расширение и наращивание сети. (Более подробная информация об использовании утилиты System Monitor содержится в главе 19.)
- ✓ Опрос пользователей. Вы можете опросить некоторых заранее подобранных пользователей в вашей организации или собрать совещание с отдельными рабочими группами и отделами. Идея заключается в том, чтобы дать возможность работникам поделиться своими наблюдениями, соображениями и пожеланиями, относящимися к работе сети. Это даст вам отличную возможность не только оценить уровень пользовательской удовлетворенности и знаний сети, но также позволит ответить на вопрос, нуждаются ли работники в дополнительном обучении, чтобы более эффективно использовать сеть.
- ✓ **Анализ сети со стороны руководства.** Вы также должны регулярно проводить встречи с представителями руководства, чтобы выяснить, каковы их планы и ожидания в отношении обработки информации в будущем. Вы также можете оценить впечатление и мнение руководства по поводу работы сети после вашего доклада, посвященного результатам анализа, проведенного в соответствии с двумя предыдущими пунктами.

Если вы организуете подобные виды анализа и будете постоянно в курсе всех возникающих изменений и требований, вы сможете обеспечить лучшую синхронизацию сети и вашей организации. Планирование изменений и роста имеет существенное значение для современных сетей, поскольку они становятся важнейшим инструментом бизнеса, от которого зависит работа организации. Если вы будете придерживаться активного подхода к планированию развития сети, вы сможете оставаться на высоте!

Схема сети — это целая история

Ранее в этой главе мы познакомили вас с основными принципами, связанными с проектированием и созданием сети. Теперь вы представляете себе, как работает сеть. Однако поработав с сетями больше времени, вы поймете — то, *что* делают сети, совсем не так важно, как ваше *знание* о том, что они делают.

Боретесь ли вы с сетями время от времени или постоянно, вы можете открыть для себя, что ничто так не помогает разобраться и следить за тем, что происходит в сети, как *схема (map)* сети.

Это не схема, а слоеный пирог!

Называть совокупность данных, которая описывает вашу сеть, *схемой*, не совсем справедливо. Схема сети — определенно больше, чем простой чертеж, который показывает, где находятся компоненты сети, однако создание такого чертежа — отличный способ начать составление сетевой схемы. Если вы взглянете на приведенный ниже перечень объектов, которые должна содержать схема сети, вы поймете, почему эта схема больше, чем просто рисунок.

- ✓ Перечень всех компонентов сети с сопроводительной документацией.
- ✓ Перечень всего сетевого оборудования, такого как серверы и концентраторы, повторители, маршрутизаторы и т.д., с сопроводительной документацией.
- ✓ Перечень всех принтеров и другого аналогичного оборудования в сети, такого как сканеры и факсимильные аппараты, с сопроводительной документацией.
- ✓ Линии, указывающие прокладку кабелей и расположение стыков, отводов и других элементов сетевой среды.

Собираем данные для сетевой схемы

Поскольку схема сети так важна и является таким мощным средством, задержитесь здесь и сразу приступайте к делу. Будьте готовы потратить некоторое время и силы на этот проект, поскольку большая часть данных, составляющих схему сети, разбросана по разным местам.

Составление подробной схемы сети — стоящее дело. Оно многократно окупится, когда вы станете опираться на нее. В худшем случае вы узнаете много больше о вашей сети, чем желали знать (но не больше, чем вам *необходимо* знать). В лучшем случае вы узнаете свою сеть настолько хорошо, что она редко сможет преподносить вам неприятные сюрпризы, более того, в ходе составления схемы вы можете обнаружить некоторые вещи, которые требуют наладки и регулировки.

Начнем с фундамента

Если вам удастся заполучить набор архитектурных чертежей или инженерных планов вашего здания, это окажет огромную помощь. Если вам удастся отыскать какие-либо чертежи или планы, сделайте с них копии, на которые вы могли бы наносить пометки, и используйте в качестве базовой схемы. (Большинство подобных планов создавалось с использованием устаревшей системы светокопирования, чертежи в которой назывались *синькой.)*

Если установку сети выполняла специализированная фирма по установке кабельных систем, вы должны найти возможность получить копии планов кабельных соединений, которые подходят даже лучше, чем архитектурные чертежи или инженерные планы, поскольку они наверняка уже показывают пути прокладки кабеля и его количество. Это еще одна причина, по которой прокладка кабеля своими силами является не лучшим способом создания сети.

Если подобные планы недоступны, вы можете обойти комнату за комнатой и набросать соответствующую схему на миллиметровке, чтобы было легче чертить в масштабе. Не забудьте отметить местоположение машин, приблизительное положение трассы кабеля и т.д.

Все, что есть в вашей сети, должно найти отражение в схеме

Все, что заслуживает внимания или стоит денег, следует зафиксировать на вашей схеме. Вам нет нужды вдаваться в подробности, касающиеся каждого коннектора, или фиксировать точную длину каждого кабеля. (Однако указание приблизительной длины в пределах метра может быть весьма полезным.) Укажите все основные трассы кабеля, каждый компьютер и каждое устройство, подключенное к сети.

Вам, скорее всего, не хватит места, чтобы зафиксировать всю эту информацию на самой схеме. Поэтому вы должны присвоить шифр машине или названию кабеля, а реальные детали зафиксировать в файле на вашем компьютере. Если вы предпочитаете использовать какой-либо собственный способ, удостоверьтесь в том, что знаете, как отыскать то, что вы зафиксировали. Какую бы схему записи вы ни приняли, следуйте ей скрупулезно. Сделайте короткие заметки, касающиеся способа организации вашей схемы записи, чтобы кто-нибудь другой смог использовать эту сетевую схему без ваших объяснений.

Проведем инвентаризацию сети

Информация, собранная вами во время составления схемы сети, образует подробную опись элементов сети и мест их расположения. К сожалению, вы вскоре обнаружите, что этой информации *слишком много.*

Чтобы облегчить себе (а также всем, кто пойдет по вашим стопам) задачу поддержания описи сети в актуальном состоянии, составьте шаблон или форму, которую вы можете заполнить для каждого элемента сети. Этот подход заставит вас собирать непротиворечивую информацию, а также легко позволит поручать сбор информации о сети кому-нибудь другому. Для каждого компьютера, входящего в сеть, включите в опись следующую информацию.

- ✓ Конфигурация **аппаратного обеспечения** для каждой машины. Включает перечень всех интерфейсов и их параметров, информацию об установленной ОП и о драйверах, марке и модели клавиатуры, дисплея и т.д. Если вы обнаружите информацию о продавце оборудования, также запишите ее.

  Учет оборудования, как правило, входит в обязанности бухгалтерии. Проведите с ними сверку наличного оборудования по копии ведомости основных фондов или описи изнашиваемого имущества (по возможности). Этот вид документации обычно включает серийные номера и другую идентификацию сетевого оборудования. Если никто в вашей компании не собирал подобную информацию, соберите ее сами. Она представляет собой большую ценность.

- ✓ **Конфигурация программного обеспечения для каждой машины.** Включает листинги конфигурационных файлов, данные операционной системы (в том числе номер версии, самый последний применявшийся пакет обновления и т.д.), а также перечень программ и версий, установленных на машине.
- ✓ **Сетевая конфигурация для каждой машины.** Включает тип и модель каждой платы сетевого интерфейса, а также перечень файлов драйверов с именами, номерами версий, датами и объемами. Вы можете легко собрать подобную информацию в файл с помощью следующей команды Windows: Start⇨Programs⇨Accessories⇨SystemTools⇨System Information⇨Hardware Resources (Пуск⇨Стандартные⇨Служебные⇨Сведения о системе⇨Ресурсы аппаратуры); она может служить вам основой описи. (В системах Windows XP и Windows Server 2003 выбор меню начинается с команды Start⇨All Programs (Пуск⇨Все программы).)

Помимо информации о каждом компьютере, ваша опись должна также включать следующие данные.

- ✓ **Перечень остального оборудования, такого как концентраторы, маршрутизаторы и принтеры.** Включает производителя, модель, марку и серийный номер каждого компонента оборудования. Если оборудование включает модули памяти, дисковые устройства или сменные карты интерфейса, также получите информацию о них. Если оборудование использует аппаратно-программное или программное обеспечение, зафиксируйте его наименование, версию, дату выпуска и любую другую информацию об этих элементах, которую вы сможете раздобыть.
- ✓ **Перечень всех кабельных сегментов сети.** Присвойте каждому сегменту уникальное имя или номер и свяжите ваши записи с каким-либо типом идентификатора, который вы используете для этих сегментов. Зафиксируйте тип и марку кабеля, его длину, местоположение его концов и все существенные соединения или промежуточные пункты, которые вам, возможно, придется осматривать в будущем.
- ✓ **Перечень всех поставщиков, которые работали над вашей сетью или входящими в нее машинами.** Включает имена и телефонные номера тех, кто выполнял каждый вид работ. Это может оказаться весьма ценным ресурсом в процессе технической поддержки и устранении проблем. Со временем добавляйте к этому перечню имена и номера телефонов специалистов по технической поддержке и других специалистов из их организаций, которые зарекомендовали себя знающими и полезными людьми.

По существу, информация, собираемая в процессе создания и сопровождения схемы сети, формирует базу данных обо всем, что требуется знать всем, кто имеет отношение к сети, Чтобы усовершенствовать доступ к этим данным и повысить удобство их использования, рассмотрите возможность хранения текстовой информации к вашей сетевой схеме в примитивной базе данных. Если этот подход неприемлем для вас, данные можно хранить в файлах или на бумаге, однако это требует больших усилий при сопровождении. Независимо от того, какой метод фиксирования данных для вашей схемы вы будете использовать, вы должны позаботиться о том, чтобы ваша опись была полной и актуальной.

Такие приложения, как Visio и HP OpenView, помогут вам при создании сетевой схемы. Чтобы найти другие приложения или компании, которые могут оказать вам помощь в этом процессе, воспользуйтесь вашим излюбленным поисковым Web-сервером, указав для поиска ключевые слова *network map* (схема сети).

Когда сеть изменяется, изменяется и схема!

Когда речь идет о сетях, вы можете всегда быть уверены в одном: они всегда изменяются. Качество вашей схемы не может быть выше качества информации, которую она содержит. И схема остается полезной до тех пор, пока эта информация является точным отражением реальной сети вашей организации.

Если в вашей сети происходят какие-либо изменения, важнейшей задачей является обновление схемы и связанной с ней базы данных. Сидеть и сверять схему намного легче, чем ходить и смотреть на реальные объекты, которые показаны на схеме. Если схема отражает текущее положение дел, вы можете чувствовать себя в высшей степени уверенно в своем офисе. Если она устарела, вам лучше начинать обход!

Глава 6

Установка сетевых адаптеров

В этой главе...

- Свой сетевой адаптер нужно знать в "лицо"
- Добываем шину
- Знакомство с расширенными возможностями адаптера
- Установка сетевого адаптера
- Проверка краевых разъемов и заглушек
- Настройка устаревших адаптеров
- Испытание результатов
- Борьба с драйверами устройств
- Подключение адаптера
- Как справиться с проблемами адаптера

Итак, пришло время подключить сеть к вашей будущей системе Windows Server 2003.

Для большинства ПК, независимо от того, работают ли они под управлением Windows Server 2003 или другой операционной системы, сетевой интерфейс (или интерфейсы, если машина имеет больше одного сетевого соединения) выступает в роли *платы сетевого интерфейса,* известного также как сетевой адаптер. Сетевые адаптеры обеспечивают необходимую связь между сетевой средой и компьютером, которому требуется доступ к сети.

В этой главе вы узнаете об основных типах, функциях и возможностях адаптеров, а также о том, как правильно выбрать тип адаптера для использования в вашем сервере. По ходу дела у вас есть возможность познакомиться с многочисленными советами и приемами, касающимися надлежащей настройки этих крайне важных компонентов.

Как адаптироваться к сети

Типичный сетевой адаптер представляет собой встраиваемую плату, которая настраивается для работы в вашем ПК. Его роль заключается в том, чтобы работать по обе стороны соединения следующим образом.

- ✓ Адаптер вставляется в шину компьютера (или специальное гнездо адаптера, называемое также *слотом расширения,* или просто *слотом),* так что он может "общаться" с ЦП (или несколькими ЦП), а ЦП может "общаться" с ним. Это в значительной мере определяет важнейшую роль адаптера — он позволяет компьютеру осуществлять доступ к сетевой среде и наоборот.
- ✓ Применение адаптера для сетевого соединения (к которому подключается сетевая среда) требует внешнего разъема для установления и, некоторым образом, связи сетевой среды с адаптером. Некоторые адаптеры включают больше одного разъема, так что если вы меняете среду (или точку зрения), вам нет необходимости выбрасывать старый адаптер и вставлять новый.

✓ Ваша сетевая технология определяет детали способа доступа адаптера к сетевой среде. Существуют адаптеры для технологий Ethernet, Token Ring, FDDI и т.д. Обычно адаптер не поддерживает больше одной сетевой технологии.

На рис. 6.1 показаны все важнейшие соединения сетевого адаптера, включая разъем шины (который обеспечивает доступ сетевого адаптера к ЦП и наоборот) и интерфейс среды (который обеспечивает доступ адаптера к сетевой среде и наоборот). Разъемы среды изменяются в зависимости от сетевой технологии и используемой физической среды. Усвоив, чем вы располагаете, вы можете выбрать сетевые адаптеры, подходящие к вашей сети.

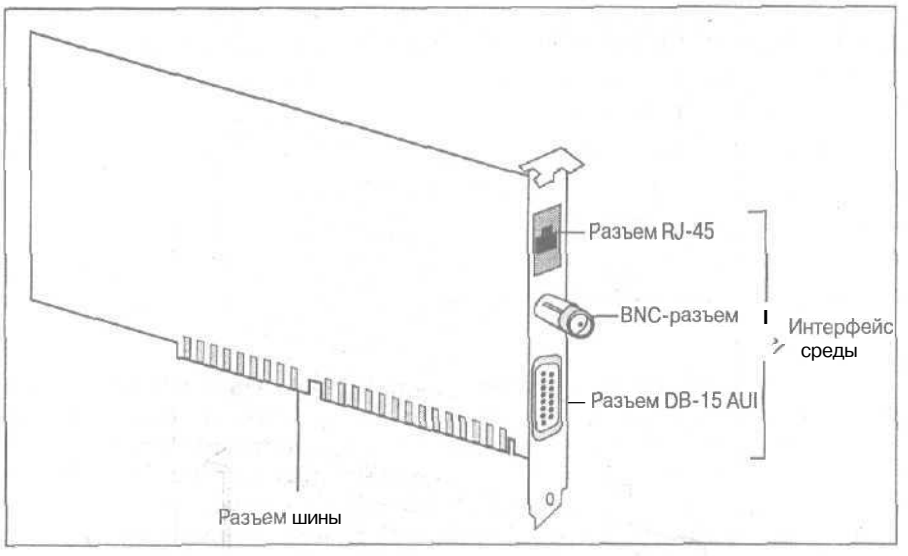


Рис. 6.1. Сетевой адаптер образует мост между компьютером и сетью

На рис. 6.1 показаны так называемая *трехвариантная комбинированная плата (three-way combo card)* для сети Ethernet с разъемом RJ-45 для *витой пары (twisted pair)* (lOBaseT), BNC-разъем для *тонкого кабеля (Thin Wire)* и разъем AUI для *толстого кабеля (Thick Wire)* (10Base5). Если это выглядит как абракадабра, не волнуйтесь — вы сможете точно узнать, что означает вся эта галиматья, в главе 7.

Не все сетевые адаптеры выступают в роли сетевой платы, которая вставляется в шину внутри компьютера. Некоторые портативные, переносные и другие виды машин не вмешают стандартный внутренний интерфейс, подобно корпусу традиционных настольных ПК. В особенности это относится к портативным ПК, в которые вы зачастую должны устанавливать платы адаптеров PC Card (ранее известные как адаптеры PCMCIA (Personal Computer Memory Card International Association — Международная ассоциация производителей плат памяти для персональных компьютеров)) в соответствии с особенностями вашей сети.

Платы PC Card весьма похожи на толстые кредитные карточки и имеют примерно такие же размеры. Вы задвигаете их в слот PC Card компьютера и выдвигаете оттуда. Иногда портативный компьютер требует адаптер PC Card для сетевого соединения в офисе и модем для удаленного доступа к сетевым ресурсам, когда владелец портативного ПК находится вне офиса.

Возьмите новейшую шину

Если ваш компьютер представляет собой настольный или серверный ПК, его сетевой адаптер (адаптеры) должен подходить к его внутренней шине (шинам) с открытым слотом (слотами). В этом разделе мы представим информацию о различных шинах, которые могут быть установлены в ваших ПК, а также расскажем, какие из них лучше других.

Рабочая часть адаптера вставляется в шину ПК и называется *краевым разъемом* (*edge connector)*. Вы можете распознать типы интерфейсов, которые включает ваш компьютер, взглянув на разъемы шины компьютера. Также взгляд на ваш адаптер может сказать вам, для какого типа шины он изготовлен. На рис. 6.2 показаны три типа шин, рассматриваемых в этом разделе, ISA, EISA и PCI, с соответствующими типами краевых разъемов.

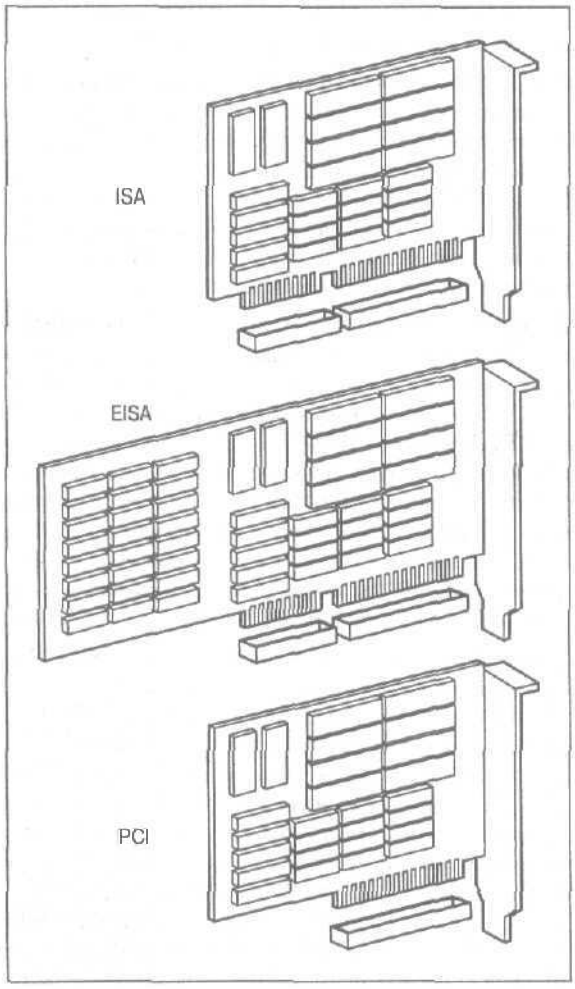


Рис. 6.2. Шины ПК и их разъемы отлично подходят друг к другу

Поскольку основная задача Windows Server 2003 состоит в обработке запросов на сетевые услуги, установите наиболее быстродействующий и мощный сетевой адаптер, который работает на вашем ПК. Теперь вы можете ожидать, что ваши сетевые клиенты будут обслуживаться с наибольшей возможной производительностью!

Сетевые адаптеры отличаются широким разнообразием, которое, в общем, соответствует архитектуре шин ПК, которые входили "в моду" и выходили из нее, начиная с 1980-х годов. Вот краткий перечень этих архитектур.

- **ISA (Industry Standard Architecture — промышленный стандарт (шинной) архитектуры).** Этот стандарт описывает шину, которая использовалась в большинстве ПК с 1985 года, когда фирма IBM выпустила компьютер типа IBM AT. Шина ISA по-прежнему остается одной из самых распространенных шин. Однако, чтобы добиться от Windows Server 2003 более высокой производительности, вам следует использовать более быстродействующую шину, такую как PCI.
- **EISA (Extended Industry Standard Architecture — расширенный промышленный стандарт шинной архитектуры).** Шину этого типа сегодня найти нелегко. Она представляет собой попытку расширить возможности шины ISA. Шина EISA обладает *обратной совместимостью* с шиной ISA, это означает, что вы можете вставить плату ISA в слот шины EISA, и она будет работать, даже несмотря на то, что платы ISA и EISA используют слегка отличающиеся разъемы (см. рис. 6.2). Хотя платы EISA обеспечивают более высокую производительность, чем платы ISA, и были разработаны специально для серверов, шина EISA так никогда и не пользовалась успехом.
- **MCA (Micro Channel Architecture — микроканальная архитектура).** Шина архитектуры MCA представляет собой 32-разрядную шину, разработанную фирмой IBM, которая обладает теми же преимуществами, что и шина EISA: высокая скорость и более широкая 32-разрядная магистраль данных. Если вы обладаете компьютером с шиной данных MCA, например ПК PS/2 фирмы ШМ, то должны приобрести адаптер MCA, чтобы работать с ним, поскольку MCA — сменная шина, а не обязательно шина расширения. Основное преимущество шины MCA состоит в том, что вы, как правило, можете вставить адаптер, после чего он управляет своей собственной конфигурацией. Это удобство, однако, не дается даром — адаптеры MCA стоят дороже других адаптеров. Шины MCA сегодня встречаются редко, за исключением мощных машин IBM типа рабочих станций на RISC-процессорах или машин AS/400.
- VLB (VESA **Local Bus — локальная шина** VESA). VESA означает *Video Electronics Standards Association (Ассоциация по стандартам в области видеоэлектроники)*. Шины VLB изготовлены по 32-разрядной шинной технологии, обеспечивающей скорость до 66 МГц. Слот VLB использует один 32-разрядный слот MCA и еще один слот стандарта ISA, EISA и MCA. Это позволяет производителям разрабатывать адаптеры, которые одновременно используют локальную и стандартную шину. Шина VLB поддерживает технологию ведущего модуля шины, известную как технология *управления шиной (bus mastering)*, которая позволяет плате брать на себя управление шиной и освобождать ЦП для обработки других задач, и за счет этого увеличивать общую производительность системы. Поскольку шина VLB зависит от стандарта MCA, она в значительной мере устарела. Отыскать новую систему с шиной VLB — трудная задача.
- **PCI (Peripheral Component Interconnect — взаимное соединение периферийных компонентов).** Шина PCI, разработанная корпорацией Intel, обеспечивает высокоскоростную магистраль данных между ЦП и периферийными устройствами (число

которых может доходить до десяти), в то время как сосуществует с платами ISA и EISA (так же как и другие шины расширения). Аналогично шине VLB, шина PCI поддерживает управление шиной, освобождая процессор для других задач. При работе с шиной PCI вы вставляете платы ISA или EISA в их обычные слоты, а высокоскоростной контроллер PCI — в слот PCI. Шина PCI поддерживает 32- и 64-разрядную реализацию с тактовой частотой до 100 МГц и скорость обмена данными до 132 Мбит/с. Не удивительно, что шина PCI до определенной степени выиграла войну шин и стала предпочтительной локальной шиной ПК. Шина PCI обеспечивает наилучшую производительность для плат периферийных адаптеров, а что касается адаптеров для серверов, — это то, что нужно.

Высокоскоростные шины наподобие EISA и PCI — отличный выбор, а вновь появившиеся стандарты, такие как *Fire Wire* (представляющая собой реализацию компанией Apple стандарта IEEE 1394) и *Fibre Channel,* — и того лучше, поскольку высокоскоростные шины превосходно удовлетворяют требованиям серверов к скорости. С другой стороны, у вас не всегда может быть достаточно средств или свободных слотов для использования высокоскоростного соединения, так что выбирайте лучшее из возможного.

Чтобы получить более подробную информацию о стандарте Института инженеров по электротехнике и электронике 1394 (EEEE — Institute of Electrical and Electronics Engineers), воспользуйтесь своим излюбленным Web-броузером, задав для поиска ключевое слово *IEEE 1394,* или исследуйте Web-узел IEEE, расположенный по адресу `www.ieee.org`.

Поскольку система Windows Server 2003 поддерживает технологии Fire Wire и Fibre Channel, возможности для создания высокоскоростных сетей на ее основе шире, чем для любой другой версии серверов Windows. Однако мы по-прежнему полагаем, что шина PCI остается лучшим вариантом с точки зрения обеспечения высокой производительности и расширенных функций, поскольку она широко доступна и поддерживается Windows 2003. Кроме того, многие поставщики предлагают адаптеры, ориентированные на шину PCI, с расширенными функциями, пригодными для использования с Windows Server 2003.

Возможно, технологии Fire Wire и Fibre Channel — лучший вариант завтрашнего дня, но сегодня конкуренция на рынке недостаточно жестока, чтобы опустить цены с заоблачных высот на землю. Вот почему мы рекомендуем приобрести самый быстродействующий PCI-ориентированный адаптер для выбранной вами сетевой технологии. Шина PCI позволит вашему серверу Windows Server 2003 работать в сети с максимально возможной скоростью, что крайне желательно для сетевого сервера любого типа.

Выбор быстродействующего адаптера для сервера

Некоторые встроенные возможности сетевых адаптеров существенно влияют на производительность сети. Низкая производительность адаптера вдвойне вредна для сервера, поскольку ограничивает доступ к его службам для всех пользователей. Фактически в сетях наподобие Ethernet, где все пользователи разделяют общую среду, медленный адаптер на любом из компьютеров однокабельного сегмента снижает полезную пропускную способность для всех пользователей сети до тех пор, пока этот медленный адаптер остается занятым.

При выборе сетевого адаптера для Windows Server 2003 начните с определения сетевой среды и разъема, к которому должна подходить плата. Это означает установление типа ис-

пользуемой технологии и принятие решения по типу разъема, который должен обеспечивать адаптер. После разрешения этих основных вопросов вы должны принять во внимание многие другие возможности адаптера, чтобы повысить скорость платы и возможности обработки данных. Поскольку производительность сервера — решающий фактор, вы повышаете общую производительность сети за счет скоростных возможностей адаптера.

Любая плата адаптера, которую вы приобретаете для использования на машине Windows Server 2003, обладает приведенным ниже перечнем возможностей (вам, может быть, не удастся найти адаптер, поддерживающий все эти возможности, но вы должны стремиться заполучить их максимальное — и приемлемое с точки зрения стоимости адаптера — количество).

- **Управление шиной.** Позволяет сетевому адаптеру контролировать шину компьютера, так что он может инициировать передачу данных в память компьютера и обратно и управлять ей. Управление шиной позволяет ЦП концентрироваться на других задачах. Управление шиной позволяет добиться повышения производительности в большей степени, чем все упомянутые здесь пункты, и может увеличить производительность сети на 20–70%. Хотя платы с управлением шиной стоят дороже адаптеров, не обладающих этим свойством, они весьма важны для работы серверов.
- **Прямой доступ к памяти.** Позволяет адаптеру передавать данные прямо из буферов встроенной памяти в основную ОП компьютера, не требуя вмешательства ЦП в этом обмен. Прямой доступ к памяти может повысить производительность на 26%.
- **Встроенный сопроцессор.** Сопроцессоры — это ЦП, встроенные в сам адаптер. Они позволяют адаптеру обрабатывать данные, не вовлекая в этот процесс ЦП. Большинство современных адаптеров включает сопроцессоры для повышения производительности сети, так что оценить их общий вклад в повышение производительности довольно трудно.
- **Буферизация памяти.** Предусматривает снабжение адаптера дополнительной ОП, которая обеспечивает область хранения для входящих и исходящих данных. Дополнительная буферизация повышает производительность сети, поскольку позволяет адаптеру обрабатывать данные с максимально возможной скоростью без вынужденных пауз на освобождение и заполнение буферов.
- **Поддержка возможностей Plug-and-Play.** Одной из наиболее сильных сторон системы Windows Server 2003 по сравнению с более ранними версиями ОС Windows NT является усовершенствованная поддержка архитектуры Plug-and-Play, предложенная Microsoft, Архитектура "Plug-and-Play" ("включай и работай") означает, что вы можете вставить устройство в ПК и оно с готовностью — и корректно — само настроит свою конфигурацию. Хотя это не дает преимуществ в производительности, мы упоминаем здесь эту технологию как существенную возможность, поскольку она повышает продуктивность *вашей* работы за счет предельного сокращения времени установки устройств. Более ранние серверы Windows зачастую требовали невероятных ухищрений, чтобы добиться установки и функционирования устройств. Для установки под Windows 2003 адаптера или другого устройства, ориентированного на технологию Plug-and-Play, часто требуется всего лишь один щелчок мышью!
- **Разделяемая память адаптера.** Использование этой возможности приводит к непосредственному отображению буферов адаптера в адреса памяти компьютера. Это позволяет "обмануть" компьютер, который "думает", что записывает данные в свою собственную память, в то время как в действительности он осуществляет доступ к буферам адаптера. Другими словами, компьютер трактует память адаптера как свою собственную ОП.

- ✓ **Разделяемая системная память.** Эта возможность по смыслу противоположна вышеприведенной и позволяет встроенному процессору адаптера записывать данные в область ОП компьютера так, будто это буферная память адаптера. Это позволяет адаптеру трактовать ОП компьютера как свою собственную и может быть предпочтительнее разделяемой памяти адаптера, поскольку позволяет ему управлять памятью и освобождает при этом процессор для других задач.

С ростом объемов сетевого трафика значение этих возможностей быстро возрастает. При выборе адаптера для вашего сервера приобретайте самый быстродействующий адаптер, поддерживающий технологию Plug-and-Play, какой только можете себе позволить. Вкладывайте средства в 32-разрядный адаптер, поддерживающий технологию Plug-and-Play, который использует либо разделяемую память адаптера, либо разделяемую системную память и включает добавочную буферную область — и вы не будете разочарованы.

Подготовка к установке адаптера

Прежде чем вы начнете копаться внутри вашего компьютера, как следует подготовьтесь. Небрежное обращение с вашей системой вполне может вывести ваш компьютер из строя — или, что еще хуже, вывести из строя вас! Если вы предпримете некоторые предупредительные шаги в начале, вы сможете предотвратить разного рода проблемы и наверняка скорее вернуться к работе.

Существуют два способа установки адаптера. При удачном варианте ваш совершенно новый сетевой адаптер удобно устроится в вашем ПК, при этом он будет делать только то, что ему положено. В противном случае он возвратится в свою упаковку, готовый к замене на что-то более подходящее, что, как вы теперь знаете, вам *действительно* необходимо!

Вот некоторые советы, способные, как нам кажется, обогатить ваш опыт установки адаптеров.

- ✓ **Прежде чем открыть ПК, отключите его от сети.** Электричество — ваш друг, но не стоит входить с ним в личный контакт. *Никогда, никогда, никогда* не открывайте ПК, который включен в розетку. Из-за этой ошибки вы или ваш компьютер (или оба) можете поджариться.
- ✓ **Если вы не можете продвигаться вперед, убедитесь в том, что вы можете вернуться назад.** Иногда после того, как вы установите адаптер и включите компьютер, вы можете получить большой, потрясающий пшик! В худшем случае вам может потребоваться отправить компьютер профессионалу для починки. В не таком уж плохом (и более распространенном) случае, если вы снимите новое устройство и аннулируете все изменения, которые вы внесли в ПО, вы вернетесь туда, откуда начали.

  Вы спрашиваете, что значит аннулировать изменения в ПО? Ответ на этот вопрос подводит нас к тому крайне важному действию, которое вы должны предпринять прежде, чем прикасаться к аппаратуре. *Прежде* всего сделайте резервную копию всех систем, которые могут быть затронуты. Резервное копирование дает два важнейших преимущества. Во-первых, если предположить, что случится самое худшее и компьютер перестанет работать, вы сможете установить вашу резервную копию на другую машину с аналогичной конфигурацией и продолжать работать, пока первый компьютер будет в ремонте. Во-вторых, если новое устройство не работает, вы можете использовать резервную копию для восстановления машины до первоначального состояния, в котором она предположительно находилась до вашего вмешательства.

Прежде чем дать "задний ход" на машине, которую вы повергли в коматозное состояние, подключив новое устройство, попробуйте воспользоваться опцией восстановления последней удачной конфигурации (Last Known Good Configuration — LKGC). (Чтобы воспользоваться этой опцией, при перезапуске Windows нажмите клавишу <F8> и выберите из меню параметр Last Known Good Configuration. — *Прим. перев.*) Эта опция осуществляет откат последних изменений реестра Windows 2003 и может позволить вам продолжить работу. Однако, подобно другим нашим наихудшим сценариям, ключом к использованию опции LKGC служит наличие удачной конфигурации реестра. Убедитесь в том, что вы перегружаете компьютер, когда он вновь нормально работает, тогда сохраненная версия реестра должна поддерживать ваш компьютер в рабочем состоянии.

- ✓ Разберитесь, с чем вы имеете дело. Когда вы добавляете еще один интерфейс в уже набитую машину, ПК может превратиться в минное поле. Если у вас нет описи установленных компонентов, а также соответствующих данных конфигурации, тотчас же подготовьте этот список. Это ускорит работу по установке и поможет вам избавиться от страха за конфигурацию. Время — деньги, поэтому помните, что на переделку всегда уходит больше времени, чем на то, чтобы все сделать правильно с самого начала.

  Одно из многих преимуществ встроенной поддержки технологии Plug-and-Play в системе Windows Server 2003 состоит в том, что всякий раз при перегрузке системы она проходит этап, который называется *этапом перебора (enumeration phase)*. Этот этап также имеет место, когда новое устройство добавляется к системе или существующее устройство удаляется из системы. Это означает, что Windows 2003 следит за устройствами в системе и может даже поддерживать изменения, которые происходят в процессе функционирования системы. Большее значение это имеет для портативных ПК, где платы PC Card могут добавляться и удаляться в процессе работы системы, чем для серверных машин, где для того, чтобы добавить или удалить карту интерфейса, вам необходимо остановить сервер.

Так или иначе, с помощью Windows 2003 вы можете заглянуть в папку Hardware Resources (Ресурсы аппаратуры) утилиты Computer Management (Управление компьютером) для получения текущего списка устройств и соответствующих параметров настройки любой машины, работающей под управлением Windows Server 2003. (Для этого воспользуйтесь следующей последовательностью команд: Start⇨All Programs⇨Accessories⇨System Tools⇨System Information⇨Hardware Resources (Пуск⇨Программы⇨Стандартные⇨Служебные программы⇨Сведения о системе⇨Ресурсы аппаратуры).)

- ✓ Оставляйте себе пространство для маневра. Освободите себе некоторое рабочее пространство. Найдите какие-нибудь бумажные стаканчики или другие небольшие емкости для хранения винтов и разъемов. Если вы действительно стали что-то разбирать, пометьте, что куда входит, чтобы исключить гадание при повторной сборке. Также убедитесь, что у вас есть надлежащие инструменты для работы. Сходите в компьютерный магазин и купите один из универсальных наборов инструментов для компьютера, которые продаются в стильных футлярах на молнии.

Когда вы ходите по ковру или находитесь в сухом помещении, вы становитесь источником статического электричества. Поэтому всегда переносите адаптеры в антистатической упаковке. До того как вы проникнете внутрь машины или начнете работать с оборудованием, обеспечьте заземление. Чтобы рассеять статический заряд, используйте антистатический манжет или наконечники. Также храните непроводящие материалы (такие как одежда из полиэстера или пенопластовые элементы упаковок) вдали от электронных компонентов. Эти материалы способны быстро генерировать статические заряды.

- ✓ **Изучите** характер вашей локальной сети. Постепенно вы подключите все установленные адаптеры к сети. Умение настраивать конфигурацию включает знание имен и адресов других серверов, пользователей и сетей, входящих в ваше окружение. Перед началом прочтите требования по установке, предоставляемые производителем сетевого адаптера, и внимательно изучите все детали, которые могут вам потребоваться во время установки. Это избавит вас от необходимости останавливаться посреди процедуры, чтобы восполнить недостающую информацию. Вложите средства в предупреждение болезни, что позволит избежать дорогостоящего и длительного лечения.

Берегите "золотые пальчики"!

Чтение руководств по материнским платам или адаптерам от иностранных производителей дает вам уникальную возможность понять, какие причудливые формы может иногда принимать английский письменный язык для тех, кто плохо знаком с ним. Например, одна тайваньская компания описывает краевой разъем (часть сетевого адаптера, которая вставляется в гнездо шины ПК) как "золотые пальчики".

Хотя эти "пальчики" скорее латунные, чем золотые, убедитесь в том, что они плотно сидят и обеспечивают надежный контакт, когда вы вставляете адаптер в пустое гнездо шины. Другими словами, убедитесь в том, что краевой разъем не виден и сетевой интерфейс со стороны карты надлежащим образом расположен в установочном отверстии на задней панели корпуса ПК. Не заталкивайте краевой разъем в гнездо шины компьютера; если требуется, осторожно покачайте его из стороны в сторону. Слишком большое усилие может привести к тому, что "золотые пальчики" оторвутся; если это случилось, вам необходима другая плата.

Вам также необходимо привинтить металлическую планку адаптера на место, используя винт, которым крепится заглушка (рис. 6.3), до ее удаления.

Рис. 6.3. Заглушки закрывают пустые гнезда и защищают компьютер от пыли и грязи

Вам не составит труда придерживаться следующих двух правил при работе с заглушками.

- ✓ Будьте аккуратны с маленькими винтиками, которые крепят заглушку. Если вы уроните винт, то, чтобы без труда обнаружить его, вам придется поднять корпус и осторожно покачать его взад и вперед. Никогда не пользуйтесь намагниченной отверткой, чтобы поднять винт, который вы уронили; иначе данные в вашем компьютере могут "свихнуться".
- ✓ Положите заглушку в коробку для инструментов или в ящик для запасных частей, чтобы позже вы могли без труда найти ее. Если вам когда-нибудь придется вынуть из компьютера адаптер (или другие платы), вам потребуется заглушка, чтобы вновь закрыть корпус. В некоторых корпусах используются нестандартные заглушки, поэтому, чтобы облегчить себе жизнь, позаботьтесь о том, чтобы нужная заглушка была у вас под рукой.

Устаревшие конфигурации адаптеров

Если вам настолько повезло, что ваш ПК, на котором установлена система Windows Server 2003, включает только платы адаптеров, поддерживающие технологию Plug-and-Play, вы, возможно, можете пропустить этот раздел с некоторой долей превосходства. Ваш адаптер сам настроит свою конфигурацию без вашего вмешательства, но если при попытке добавить адаптер (или некоторое другое устройство) к системе Windows Server 2003 вы столкнетесь с проблемами конфигурации аппаратных средств, вам все же может потребоваться ознакомиться с этим материалом.

Настройка конфигурации сетевого адаптера для Windows 2003, несовместимого со стандартом Plug-and-Play, требует как правильного выбора аппаратных настроек, так и подбора соответствующих программных установок. Короче говоря, вам придется иметь дело с многочисленными установками и предоставить программным драйверам адаптера верную информацию по конфигурации. Хотите узнать ужасные подробности — читайте дальше!

Адаптеры просят прерываний

Потребность в сетевом взаимодействии может возникнуть в любой момент. Чтобы получить входящие данные и обработать исходящий поток, адаптер должен быть в состоянии подать ЦП или шине сигнал (для входящего потока) или, наоборот, получить сигнал от них (для исходящего потока).

Самым распространенным способом справиться с подобной ситуацией является резервирование *запроса на прерывание (interrupt request — IRQ)*, которым мог бы пользоваться адаптер. Обычно ПК поддерживает 15–23 IRQ, которые нумеруются последовательно от 0 до 15 или 23, в зависимости от количества установленных контроллеров прерываний. Интерфейсы используют запросы на прерывания для сигнализации о некотором действии. Каждый адаптер должен обладать своим собственным уникальным значением IRQ в диапазоне, который способна обработать сетевая карта.

Эти величины помогают понять, почему создание схемы конфигурации ПК — полезное дело. Ваша задача, нравится вам это или нет, заключается в том, чтобы найти IRQ, которые не используют другие адаптеры и которые получит в свое распоряжение ваш новый адаптер. Если подобное IRQ отсутствует, вы должны внести изменения в другой адаптер, чтобы освободить подходящий IRQ. Для адаптеров, работающих с шиной PCI, — это несложная задача, поскольку она сама обрабатывает запросы на прерывания.

Обычно установка IRQ означает выполнение программных установок, установку DIP-переключателей *(DIP* означает *dual-in-line package — корпус (микросхемы) с двухрядным расположением выводов)* или перестановку перемычек. Что касается программных установок, то они самодокументируемы, а вот как использовать DIP-переключатели и перемычки, мы объясним вам в следующем разделе.

Как правильно выставить DIP-переключатели

Большинство *DIP-переключателей,* которые фактически представляют собой пакеты отдельных переключателей, указывают, какие пути сигналов открыты, а какие закрыты. Если вам не у кого спросить, как выставить переключатели, а руководство по установке адаптера мало в чем помогает, тотчас же обратитесь в подразделение технической поддержки поставщика (или узнайте, имеется ли у него Web-узел). Поставщик должен знать ответ, и это предохранит вас от ненужных и потенциально опасных догадок или экспериментов. На рис. 6.4 показан типичный DIP-переключатель. DIP-переключатели можно встретить в ISA-адаптерах; в PCI-адаптерах вы их не найдете.

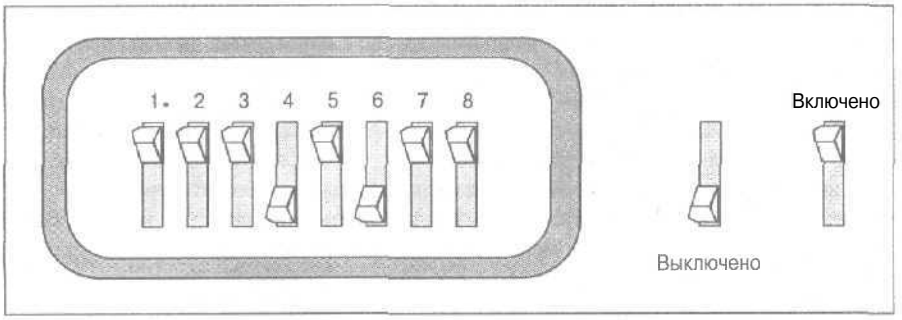


Рис. 6.4. Зачастую DIP-переключатели управляют различными установками адаптеров

Такие забавные и такие важные перемычки!

Блоки перемычек состоят из двух рядов смежных контактов, связанных с крошечными приспособлениями, называемыми *перемычками (jumper)* (рис. 6.5). Контакты пронумерованы буквой J, за которой следует номер (например, J6).

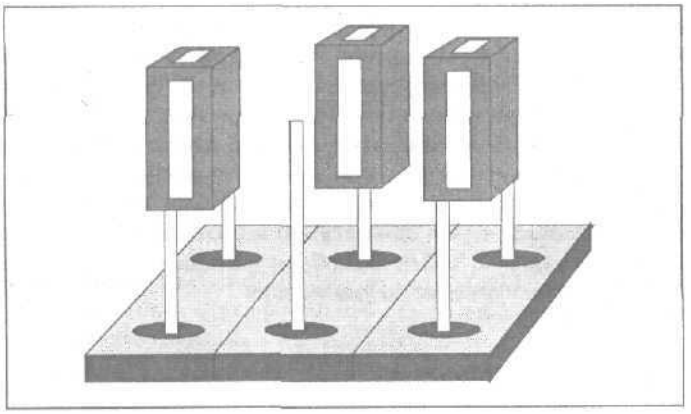


Рис. 6.5. Типичный блок перемычек состоит из нескольких контактов с отдельными перемычками

Если одеть перемычку на оба контакта, то перемычка включена. Для отключения пронумерованного набора контактов снимите перемычку с обоих контактов и оденьте ее на один из двух контактов так, чтобы она выступала за контактный блок (как в среднем положении на рис. 6.5). Зачастую, когда вы устанавливаете IRQ с помощью перемычек, вы вставляете одну перемычку для всего блока контактов. Набор контактов, соединенных перемычкой, соответствует одному выбранному IRQ. В этом случае вы должны убедиться в том, то перемычка плотно сидит на обоих контактах.

Смотрите, не забудьте про умолчание!

Прежде чем вы начнете проявлять чрезмерное беспокойство о DIP-переключателях и перемычках, проверьте руководство по установке адаптера, чтобы выяснить, не установил ли производитель IRQ по умолчанию. Если производитель предусмотрел установки по умолчанию, вы можете придерживаться их и больше ничего не предпринимать. Когда такое случается, считайте, что вам повезло!

Входим в порт приписки

Каждая плата в системе обладает уникальным адресом порта ввода-вывода, причем для конкретных интерфейсов, в особенности видеоадаптеров, зарезервированы определенные адреса. Сетевые адаптеры в этом отношении довольно привередливы и, как правило, получают адрес порта ввода-вывода из диапазона адресов, зарезервированных для использования ими. В общем случае этот адрес устанавливается программно или с помощью DIP-переключателя для большинства адаптеров, поскольку возможный диапазон установок довольно широк.

Порт ввода-вывода позволяет компьютеру осуществлять считывание и запись в память, которая принадлежит интерфейсу. При появлении сигнала прерывания компьютер получает указание выполнить операцию чтения или записи в порт ввода-вывода. Информация, записанная или считанная из адреса порта ввода-вывода, переписывается по шине между адаптером и ЦП.

Можем ли мы говорить прямо? Установка DMA

Некоторые адаптеры используют метод, называемый *прямым обращением к памяти (direct memory access),* для передачи информации между адаптером и ЦП. Этот метод ускоряет переписывание информации из компьютера в адаптер и наоборот. Этот метод утратил свою актуальность (и стал менее распространенным) из-за увеличения скорости работы компьютеров и оборудования.

Метод DMA устанавливает соответствие между двумя областями памяти: одна из них принадлежит компьютеру, а вторая — адаптеру. Запись данных в область памяти компьютера вызывает автоматическое переписывание данных в область памяти адаптера и наоборот. Установление DMA-адреса означает поиск незанятого блока DMA-памяти, чтобы назначить его вашему адаптеру, И вновь, как и в случае вашего более раннее исследования, связанного с назначением IRQ, выяснение того, какие значения установочных параметров уже заняты, поможет вам избежать конфликтов. Выберите незанятый блок адресов и выполните надлежащие установки для адаптера, чтобы привести его в соответствие с остальными. Если вы обнаружите конфликт, вам следует найти способ его разрешения. Также помните о необходимости проверить установки, принятые по умолчанию.

MemBase — это не новая молодежная группа

Сетевой адаптер содержит свою собственную память, которая называется *буферной областью (buffer space)*; эта память обеспечивает рабочую область для запоминания информации, поступающей из сети и отправляемой в сеть. Буферной области необходимо назначить эквивалентную область в памяти ПК, называемую *базовым адресом памяти (memory base address)*, или *MemBase.*

Как и в случае IRQ и DMA, эта установка должна быть уникальной. Остерегайтесь потенциальных конфликтов адресов и старайтесь разрешить их. Если программное обеспечение не выполняет установок MemBase на вашем компьютере автоматически, то вы можете воспользоваться перемычками. К общим значениям установок MemBase для адаптеров относятся адреса COOOh, D000h и D800h.

Если адаптер входит в перечень совместимого оборудования фирмы Microsoft (Microsoft Hardware Compatibility List — HCL), его возможная конфигурация, вероятно, также приведена здесь (`www.microsoft.com/hwdq/hcl/`), так что вам не придется все выяснять самостоятельно. Также позаботьтесь о том, чтобы проверить установочное ПО адаптера перед тем, как устанавливать Windows 2003, если вам необходимо найти драйвер для сетевой платы (как это сделать, мы объясняем в следующем разделе).

Драйвер занимает свое место

После установки устройства адаптера вы должны решить проблему программного драйвера устройства. Если ваш адаптер — новая модель, для него лучше всего использовать драйверы, включенные в диск, поставляемый с устройством.

В этом случае (вероятность которого мы оцениваем равной шансам выиграть в лотерею) вы можете загрузить диск, запустить программу установки, подставить кое-где необходимые значения и приготовиться танцевать рок-н-ролл. Если вы не такой счастливчик, вам придется охотиться за драйверами самому.

Наш совет: прежде чем устанавливать драйвер, всегда определите его последнюю и наиболее усовершенствованную версию. За помощью лучше всего обращаться в следующем порядке.

1. В компанию, которая продала вам адаптер.
2. В компанию, которая разработала сетевую карту.
3. По Internet. Для поиска адаптера по компании-производителю и модели воспользуйтесь поисковым процессором. В результате вы получите если не подходящее ПО, то полезную информацию.

Подключение сетевого адаптера к кабелю

Итак, ПО установлено и устройства вставлены. Все, что осталось сделать, — это подключить адаптер к сети. Для модульных технологий наподобие Ethernet на основе витой пары или Token Ring это означает вставить модульный разъем кабеля ЛС в гнездо адаптера. Для других технологий это означает подключить Т-коннектор или кабель трансивера ЛС к адаптеру. В любом случае убедитесь в том, что соединение надежно и адаптер прочно сидит в своем гнезде. Теперь вы готовы к запуску!

Когда проблемы ftfte&teqtftoiH tfac, будьте готовы к отпору!

Вы преодолели лабиринт потенциальных конфликтов адресов и задали подходящие значения установочных параметров для адаптера. ПО установлено, так что все должно работать, не правда ли? Обычно так и бывает (громкие поздравления и победно поднятый кулак), но иногда бывает и иначе (серьезный разнос и зубовный скрежет). Существуют четыре признака, по которым можно понять, что что-то не в порядке.

- ✓ **ПК не загружается.** Этот случай очевиден. Если вы не можете загрузиться, самое время отменить все только что выполненные вами действия. Сначала восстановите систему до состояния, в котором она находилась до того, как вы начали шуровать с оборудованием (т.е. удалите все вновь установленные устройства и кабельные соединения). Если это срабатывает, значит, проблема заключается в новом оборудовании (адаптере). В противном случае — у вас большие проблемы. Время посетить ремонтную мастерскую.
- ✓ **ПК загружается, но не подгружает драйверы.** Ниже перечислены наиболее распространенные причины, по которым драйверы не загружаются.
  - **Неплотное соединение.** Убедитесь в том, что кабель плотно и надежно вставлен в адаптер и на другом конце он к чему-то подключен.
  - **Проблемы с установкой.** Убедитесь в том, что драйверы расположены в соответствующем каталоге и что на этот каталог имеется ссылка в вашем загрузочном файле или же он определен в операторе PATH. Поскольку система Windows 2003 активно сканирует ваш жесткий диск в поисках драйверов, для машин, работающих под управлением Windows Server 2003, это обычно не проблема (при условии, что ваш адаптер входит в перечень HCL).
  - **Конфликт.** Вы могли что-нибудь упустить и внесли конфликт. Проверьте все другое оборудование; если еще что-то также отказывается работать, это страшное предательство. Время вернуться в самое начало и перепроверить все системные установки.

    Единственным положительным моментом здесь можно считать то, что подобная проблема, скорее всего, является результатом неплотного соединения или просчета в конфигурации. Если причины не в этом, придется нанести визит в ремонтную мастерскую!
- ✓ **ПК загружается частично, а затем зависает с появлением синего экрана.** Иногда Windows 2003 начинает загружаться, но зависает с появлением темно-синего экрана, заполненного текстом белого цвета, который начинается с кода ошибки. Среди приверженцев Windows это явление получило название "синего экрана смерти". Если подобное явление возникает при установке, оно обычно связано с некоторыми проблемами с драйверами устройств. Но что значит, если оно возникает сразу после установки адаптера, а Windows 2003 была загружена перед этим? Это свидетельствует о том, что установленный вами драйвер адаптера не работает надлежащим образом и должен быть заменен работающим драйвером. Позаботьтесь о том, чтобы в вашем распоряжении был самый последний и наиболее усовершенствованный драйвер. Если вы испытываете затруднения, отправьте поставщику сообщение по электронной почте или вызовите бригаду технической поддержки. Если эта проблема возник-

ла при начальной установке Windows 2003, может быть неясно, что вызвало проблему. В этом случае обратитесь *к* главе 22, в которой содержатся советы по установке и настройке конфигурации.

- ✓ Вы пытаетесь использовать сеть, а она отказывается отвечать. Это хитрый вариант проблем с драйвером адаптера, и его вызывает одна или несколько аналогичных причин. Здесь вам придется призвать на помощь все ваши детективные способности, потому что причиной конфликта может быть скорее приложение, чем драйвер. Либо сеть может блокироваться неверными установками для адаптера, либо неверной сетевой конфигурацией, либо неправильным паролем для входа в систему (т.е. ПО работает нормально, но вы пытаетесь заставить его неверно себя вести). Чтобы найти ответ, вам следует осторожно пройти весь процесс исключения одного варианта за другим. Удачи вам, и почаще делайте перерывы. Помните, что нет ничего зазорного в том, чтобы попросить помощи!

После того как вы преодолели все препятствия и можете взаимодействовать с сетью, вы готовы приступить к работе. Если же вы — начинающий сетевой администратор, вы будете иметь удовольствие помочь кому-нибудь впервые начать работать с сетью. Так или иначе, пущенная вами сетевая волна устремилась вперед, к другим машинам!

Глава 7

Подключение сети

В этой главе...

- Выбор подходящей сетевой среды
- Выбор технологии Ethernet
- Знакомство с сетевой магистралью
- Сеть или объединенная сеть
- Выход в мир: работа с глобальной сетью

Купить компьютеры еще не значит создать сеть! Необходимо соединить компьютеры между собой, чтобы дать им возможность взаимодействовать. Существует несколько способов установить взаимодействие компьютеров; вы выбираете подходящий исходя из возможностей вашего бюджета и потребностей в пропускной способности сети. Ну ладно, вы правы, по большей части все зависит от вашего бюджета!

Передающая среда (transmission media) — модный общий термин для кабельных и беспроводных систем передачи сообщений. Среда служит средством, с помощью которого компьютеры общаются друг с другом по сети. Фактически компьютеры могут взаимодействовать посредством воздушных радиоканалов, используя широковещательную передачу, с помощью проводки в зданиях и посредством волоконно-оптических кабельных систем масштаба кампусов. Подключение к локальным сетям магистральных или Internet-соединений означает, что ваша сеть обладает практически неограниченными возможностями доступа к информационным ресурсам,

В этой главе вы познакомитесь с различными методами соединения сетей с помощью кабельных систем и других типов сред. Вы выясните, какие среды подходят для настольных систем, а какие лучше работают в случае взаимодействия серверов. Вы также узнаете больше о структуре сетей по мере того, как мы станем прорабатывать две темы, а именно: магистральные каналы и глобальные сети.

Выбор подходящей сетевой среды

Выбор подходящей сетевой среды означает реализацию такой сетевой кабельной системы, в которой не возникает узких мест. В зависимости от того, создаете ли вы сеть с нуля или расширяете существующую, вам могут потребоваться различные подходы к оцениванию вариантов монтажа кабельной проводки для вашей сети.

- ✓ Если вы начинаете работу, когда локальная сеть (ЛС) уже существует, то для нее, скорее всего, существует и кабельная проводка. В этих условиях, пожалуй, лучшее, что можно сделать, — это оценить тип, возможности и пригодность унаследованной сети. Таким образом, вы можете оставить все без изменений или же внести некоторые изменения, призванные улучшить сеть. Вы можете, например, выяснить, что старая кабельная проводка вызывает столько проблем, что вам лучше заменить или реконструировать ее. (Мы вскрыли подвесной потолок и обнаружили скрытые от взгляда плохо состыкованные кабели.)

- ✓ Если вы планируете совершенно новую сеть, одна из ваших забот — определение требований к кабельной системе. Следует решить, какую сетевую проводку вы станете использовать *до того,* как закажете оборудование для вашей сети, поскольку может случиться так, что вы закажете компьютеры и периферийные устройства, соответствующие сетевые интерфейсные платы которых заранее установлены и сконфигурированы. (Конечно, сетевые адаптеры существующей сети уже установлены и сконфигурированы, а это означает, что выбор уже сделан за вас.) Чем больше усилий вы сэкономите, тем лучше!
- ✓ Если текущий ремонт вашей сети осуществляет подрядчик, не думайте, что он заменит все старые кабели, если они полностью не пришли в негодность. Подрядчик может пойти на то, чтобы снова использовать некачественные кабели, чтобы сэкономить на стоимости материалов. Без надлежащей проводки ваша сеть будет постоянно испытывать трудности (если вообще будет работать).

Если вы работаете с подрядчиком по кабельным системам, требуйте, чтобы он проверил каждый кабель, и настаивайте на том, чтобы предъявил вам результаты этих испытаний. В действительности многие компании нанимают одного подрядчика для прокладки кабеля, а другого — для его испытания. За счет этого они могут быть уверены, что им удастся избежать общей тенденции, связанной с незамеченными ошибками, или потенциальных проблем с сетью; кроме того, никогда не вредно выслушать еще одну независимую точку зрения.

Наиболее распространенной технологией для ЛС является сеть с *немодулированной передачей (baseband network);* такие сети называют также *однополосными сетями,* а кабель, установленный для немодулированной передачи, соответственно называется *однополосным кабелем (baseband cable).* Мы сосредоточимся на этой технологии по причине ее широкого распространения. Описанию немодулированной передачи и ее отличий от широкополосной сети посвящена врезка "Используйте подходящие "трубы" в ваших сетевых "трубопроводах".

Если вы знаете, что искать, наименование конкретного типа кабеля может рассказать вам все о его характеристиках, касающихся передачи данных. Обозначение, наносимое на кабели сетей Ethernet (установлено ШЕЕ), разделяется на следующие группы.

- ✓ Скорость сети Ethernet в Мбит/с.
- ✓ Технология кабеля — широкополосная или однополосная.
- ✓ Номинальное расстояние для кабеля в сотнях метров или тип кабеля — витая пара или волоконно-оптический кабель.

Например, 10Base5 — маркировка сети Ethernet, обозначающая: 10Мбит/с, однополосная (5 х 100 м = 500 м). Из самого наименования вы можете сказать, что узкополосный кабель рассчитан на пропускную способность 10Мбит/с на кабельный сегмент длиной до 500 метров.

Буквы *T* и F в маркировке кабельных систем означают соответственно *витую пару (twisted pair)* и *волоконную оптику (fiber-optic).* Например, маркировка *10BaseT* означает, что этот конкретный однополосный кабель Ethernet рассчитан на использование витой пары при пропускной способности 10 Мбит/с. Аналогично, *10BaseT*означает то же самое, за исключением использования волоконно-оптической среды вместо витой пары.

Используйте подходящие "трубы" в ваших сетевых "трубопроводах"

Кабельная проводка сети аналогична домашнему водопроводу. Так же как трубы образуют магистрали, по которым вода попадает в сантехнические устройства, сетевая проводка обеспечивает магистрали, посредством которых компьютеры передают данные с использованием электрических сигналов. Объем данных, который компьютеры могут перемещать через кабельную систему в единицу времени, зависит от характеристик установленных кабелей (или "труб"). Чем мощнее "трубы", тем больше данных могут пересылать по ним компьютеры.

Вы можете представить себе ***полосу пропускания*** сети как размер сетевых "труб". Полоса пропускания представляет диапазон применяемых частот и измеряется в герцах (Гц). Чем выше номинальное значение частоты для сетевой среды, тем шире располагаемая полоса пропускания. Более широкая полоса пропускания превращается в "трубы" большего объема для передачи данных. Само по себе наличие у вас больших "труб" не означает, что вы всегда заполняете их полностью. Поэтому имеет смысл измерить фактический объем данных (называемый ***пропускной способностью (throughput)***, протекающий через "трубы".

Различные типы кабелей рассчитаны для передачи различных объемов данных на различные расстояния. Следует, однако, помнить, что даже если труба достаточно велика, чтобы справиться с потоком пропускаемой по ней воды, она все равно может засориться. В результате, хотя заданный объем данных может теоретически проходить через кабель, вы можете наблюдать меньшие потоки данных, чем позволяет полоса пропускания. Водопроводчики расскажут вам, что отложения минералов и засорение зачастую могут ограничить движение воды через трубы. Продолжая нашу метафору, можем сказать, что шумы, перекрестные и электромагнитные помехи, а также другие недуги сети зачастую снижают фактическую производительность вашего кабеля. ***Пропускная*** *способность,* обычно измеряемая в битах в секунду (бит/с), описывает фактический объем данных, который проходит через кабель в единицу времени.

Если БЫ возьмете одну "трубу" и разделите ее на меньшие "трубы", вы заново откроете концепцию ***широкополосной передачи*** (при которой используется одновременная передача данных через сетевую среду на нескольких разных частотах). Если "труба" остается целой, а не разделяется, вы приходите к концепции ***однополосной*** **передачи** (при которой вся полоса пропускания используется для переноса данных только на одной частоте, при этом одновременно возможна передача только от одного узла).

Вы все усвоили? Ну что, нужно звать водопроводчика!

Сетевые кабели: есть из чего выбрать

Сетевая проводка и кабели отличаются большим разнообразием размеров и форм. С каждым типом кабеля связано ограничение по расстоянию. Каждый тип кабеля также отличается по цене, характеристикам передачи данных и др. К наиболее употребительным типам кабелей в современных сетях относятся витая пара, коаксиальный и волоконно-оптический кабель.

Витая пара

Существуют два вида кабелей типа витая пара: *неэкранированная витая пара (unshielded twisted-pair— UTP)* и *экранированная витая пара (shielded twisted-pair — STP).* Проще всего отличие экранированной витой пары от неэкранированной можно объяснить следующим образом: каждая скрученная пара проводов экранированной витой пары обвернута фольгой или проводящей оплеткой, а неэкранированная — нет.

Кабель UTP

Если в вашей организации установлена телефонная система, то вы, вероятно, видели, что собой представляет кабель UTP. Вы могли даже видеть подобную проводку внутри стен вашего дома (если наблюдали за тем, как ее устанавливают нанятые вами работники).

Кабель UTP состоит из пар медных проводов, каждый из которых заключен в пластиковую оболочку, маркированную определенным цветом. Отдельные провода скручены, и весь кабель целиком обвернут во внешнюю оболочку. На рис. 7.1 показан поперечный разрез ти-

пичного кабеля UTP. Количество скруток (витков) на единицу длины кабеля (шаг скрутки) является важной характеристикой, поскольку увеличение шага скрутки улучшает характеристики передачи проводов и повышает устойчивость кабеля к помехам. Это добавляет к витой парс целую новую скрутку!

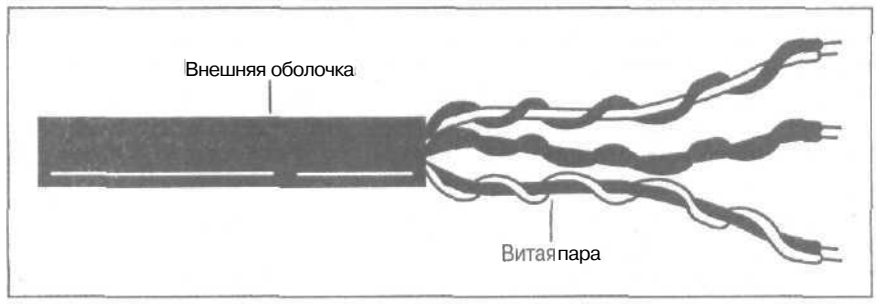


Рис. 7.1. Витая пара: скрученные пары проводов внутри оболочки

Обратите внимание на букву *U* в аббревиатуре UTP, которая указывает на то, что это *неэкранированная* витая пара *(unshielded twisted-pair — UTP)*. Это обозначение включено из-за существования еще одного типа витой пары — *экранированной (shielded twisted-pair — STP)*. Различие между этими типами кабелей состоит в том, что кабель STC включает дополнительный экранирующий слой для каждой пары скрученных проводов. В современных сетях используются оба типа кабелей, однако кабель UTP более распространен, поскольку кабель STP стоит дороже. Более подробно о кабеле STP вы узнаете ниже в этой главе.

Телефонные (или голосовые) кабели UTP (кабели категорий CAT 1 и 2 — классификация категорий кабелей приведена ниже) — это тип кабеля, установленный в большинстве домов и в старых телефонных системах. *Телефонный*, или *голосовой кабель UTP (voice-grade UTP cable)*, применяется для передачи голосовых сигналов и достаточно дешев. Когда некоторые организации обнаруживают, что в их офисах уже протянуто и заделано слишком много телефонных проводов, они стремятся использовать их в качестве сетевых кабелей. Проблема в том, что голосовой (он же телефонный) кабель не предназначен для передачи данных. Если вы обладаете небольшой ЛС с невысоким трафиком, подобный кабель может вас устроить. Однако если вы создаете большую сеть, работающую с мощными приложениями баз данных, голосовой кабель UTP неприемлем. Вам необходимо установить кабель UTP более высокой категории.

Классификация кабелей UTP, введенная Ассоциацией производителей электроники (Electronic Industry Association), основана на такой характеристике, как скорость передачи данных по кабелю. В соответствии с этой классификацией кабели UTP делятся на категории, для которых иногда применяется обозначение *CAT*. Ниже приведен текущий реестр категорий кабелей UTP, которые используются в настоящее время.

- ✓ Категории CAT 1 и 2. Используются только для передачи голоса и низкоскоростных данных.
- ✓ **Категория CAT** 3. Используется для передачи данных со скоростью до 16 Мбит/с.
- ✓ **Категория CAT 4.** Используется для передачи данных со скоростью до 20 Мбит/с.
- ✓ Категория CAT 5. Используется для передачи данных со скоростью до 100 Мбит/с.

- ✓ Категория CAT 5 (улучшенная). Используется для передачи данных со скоростью до 200 Мбит/с.
- ✓ **Категория** CAT 6. Используется для передачи данных со скоростью до 600 Мбит/с.

Кабели категории CAT 6 отличаются от своих двойников категорий CAT 1-5. Каждая пара такого кабеля экранируется фольгой, после чего весь кабель в целом также защищается слоем фольги. Это дополнительное экранирование помогает защитить кабель от шумов и других помех. Остается только ответить на вопрос: "Почему кабели UTP категории CAT 6 называются неэкранированными, если они экранированы?" Увы, некоторые острые вопросы должны оставаться без ответа!

(Заметим, что иногда в литературе по сетям встречается классификация кабелей UTP, в которой присутствуют категории с 1 по 7; при этом категории CAT 5 (улучшенной) соответствует категория 6, а категории CAT 6 — категория 7. — *Прим. перев.*)

Если в вашей сети уже используются кабели UTP и вы не уверены, к какому классу они относятся, обратитесь в специализированную фирму, чтобы они проверили, какие кабели установлены в вашей сети.

Если вы планируете установить для сети кабель CAT 5, убедитесь в том, что разъемы, используемые от одного конца сети до другого, также принадлежат классу CAT 5. Если вы проследите за каким-нибудь соединением, которое образует ваш компьютер с сетью, по всему его пути через стены и т.д., то обнаружите многочисленные компоненты, включая настенные платы, монтажные блоки и коммутационные панели. Чтобы все эти элементы сети работали как следует, с расчетной скоростью передачи данных, они должны относиться к классу CAT 5.

Кабели UTP более дешевы и более употребительны, чем кабели STP, однако они обладают некоторыми незначительными недостатками. Поскольку кабель UTP не экранирован, он подвержен влиянию помех от внешних источников, таких как люминесцентное освещение. Эти кабели часто заделываются в подвесные потолки, протягиваются по световой арматуре или вблизи лифтов. Такое расположение может привести к сетевым помехам, поэтому следует внимательно относиться к расположению кабелей.

Еще одним затратным фактором для витой пары является требование подключения рабочих станций к сети через концентратор. Хотя вы можете купить простой концентратор на восемь портов стоимостью около 50 долларов, если вы планируете создание большой сети, эти добавочные затраты также требуется принимать во внимание. Положительным моментом является преимущество, которого можно достичь за счет использования в сети *интеллектуальных концентраторов (smart hub),* поскольку они могут помочь управлять вашей кабельной системой, — однако подобная "интеллектуализация" управления сказывается на цене подобного оборудования. В конце концов, менее дорогие концентраторы всегда оснащены мигающими лампочками, которые укажут вам, какие порты активны и передаются ли данные.

В большинстве случаев вы станете использовать для своей сети кабели UTP — до тех пор, пока вам не потребуется дополнительное экранирование кабелей STC или волоконно-оптические кабели.

Большинство имеющихся в наличии сетевых адаптеров поддерживают только кабели UTP/STP (становится все труднее и труднее найти комбинированные платы, поддерживающие и кабели UTP/STP, и коаксиальные кабели). Вдобавок к этому большинство устройств для сетевых соединений наподобие концентраторов, повторителей, мостов и маршрутизаторов обладают только портами UTP/STP.

10BaseT

10BaseT — довольно известная версия технологии Ethernet, которая получила широкое распространение в современных сетях. Данный стандарт предусматривает звездообразную топологию, которая использует концентраторы, соединенные неэкранированной витой парой. Как ясно из наименования этого стандарта, присвоенного ему IEEE, сети 10BaseT рассчитаны на скорость передачи данных до 10 Мбит/с. Сеть 10BaseT требует по меньшей мере использования кабеля UTP категории CAT 3. Для сетей 10BaseT вы можете установить кабель категории CAT 5, чтобы предусмотреть переход к сети с более высокой пропускной способностью, например 100BaseT. Приведенный ниже перечень указывает, что вам может потребоваться для сети 10BaseT.

- ✓ Адаптеры. Адаптеры Ethernet с разъемами RJ-45,
- ✓ . **Кабель.** Кабель UTP категорий CAT 3-5 на промежутке от сетевого адаптера до трансивера . (если используется внешний трансивер).
- ✓ Трансивер, Может быть внешним или встроенным в сетевой адаптер.
- ✓ **Кабель.** Кабель UTP категорий CAT 3-5 на промежутке от трансивера (или адаптера) до стены.
- ✓ Настенная плата. Гнезда RJ-45.
- ✓ Кабель внутри **стены.** Кабель UTP категорий 3-5.
- ✓ **Монтажный** блок. Сюда сводятся входящие кабели UTP и обжимаются с помощью специального инструмента.
- ✓ **Кабель.** Кабель UTP категорий CAT 3-5 от монтажного блока до коммутационной панели.
- ✓ Кабель. Соединительный кабель ШР категорий CAT 3-5 от коммутационной панели до концентратора.

При реализации сети 10BaseT следует учитывать некоторые ограничения

- V- **Расстояние.** Длина кабеля от сетевого устройства до концентратора не должна превышать 100 метров.
- ✓ Узлы. В сети нельзя использовать больше 1024 узлов без разделения сети и добавления устройства маршрутизации между подразделениями.
- ✓ **Концентраторы.** Вы можете не вставлять больше 12 дополнительных концентраторов в основной концентратор, чтобы увеличить количество доступных сетевых устройств.

STP: экранирование увеличивает производительность

Как мы уже объясняли ранее, экранированная вита пара, STP, содержит дополнительный защитный слой вокруг каждой из витых пар. Этот дополнительный экран представляет собой проволочную сетку или слой фольги, расположенный между отдельными парами проводов и внешней оболочкой. Кабель STP способен передавать данные со скоростью от 155 Мбит/с на расстояние до 100 метров, однако такая реализация нетипична и довольно дорогостоящая. Обычно на основе кабеля STP реализуются сети Token Ring с пропускной способностью 4–16 Мбит/с (однако иногда используется и кабель UTP).

Наиболее вероятно обнаружить кабель STP в старых сетях Token Ring и LocalTalk, а также в старых сетях на основе мэйнфреймов IBM. Компания ШМ — оригинальный разработчик технологии Token Ring, и она до сих пор изготавливает и продает компоненты сетей Token Ring. Вот почему большинство предприятий "Голубого гиганта" используют сети Token Ring.

Кабель STP может требовать электрического заземления, а установка заземления — нешуточное дело. По сравнению с кабелями UTP кабели STP толще и менее гибкие, поэтому их труднее прокладывать и обращаться с ними. Разъемы для кабелей STP неудобны, и их не всегда легко вставлять. Кабели STP стоят дорого, поэтому, если вам не требуется более высокая пропускная способность, обеспечиваемая кабелями STP, лучше обходиться кабелями UTP, чтобы упростить установку и уменьшить расходы.

Коаксиальный кабель (коаксиал)

Коаксиальный кабель, или коаксиал, когда-то был самой распространенной средой передачи данных для сетей. Однако в связи со значительным уменьшением стоимости кабелей UTP в последние несколько лет стало трудно найти коаксиальные кабельные системы, а также рассчитанные на них адаптеры и другие сетевые устройства связи. До появления кабелей UTP в середине 1980-х годов в старых сетях использовались исключительно коаксиальные кабели. Вначале были доступны только "толстые" коаксиальные кабели (которые мы предпочитали называть "замерзшими желтыми садовыми шлангами"). "Толстый" коаксиальный кабель довольно обременителен в эксплуатации и при установке. Представьте себе прокладку замерзшего садового шланга через потолочное покрытие, а затем подключение *трансивера* (*transceiver* от transmitter-receiver — приемопередатчик) к этому кабелю! Замерзший садовый шланг проложить, наверное, легче...

Коаксиальный кабель имеет два слоя изоляции и состоит из медного провода, покрытого пластиковой изоляцией, окруженный защитным проводящим экраном в виде проволочной оплетки, которая, в свою очередь, имеет внешнюю изоляционную "рубашку". Эта "рубашка" помещена в пластиковую трубку, называемую *оболочкой (cladding)*. На рис. 7.2 показан поперечный разрез хорошо "укутанного" отрезка коаксиального кабеля.

Существует простой способ определения стоимости различных типов коаксиального кабеля. Чем больше диаметр кабеля, тем он дороже. В этом случае "больше" не обязательно означает "лучше", но определенно означает дороже. В табл. 7.1 приведена классификация коаксиальных кабелей, основанная на американской военной спецификации кабелей Radio Grade (RG).

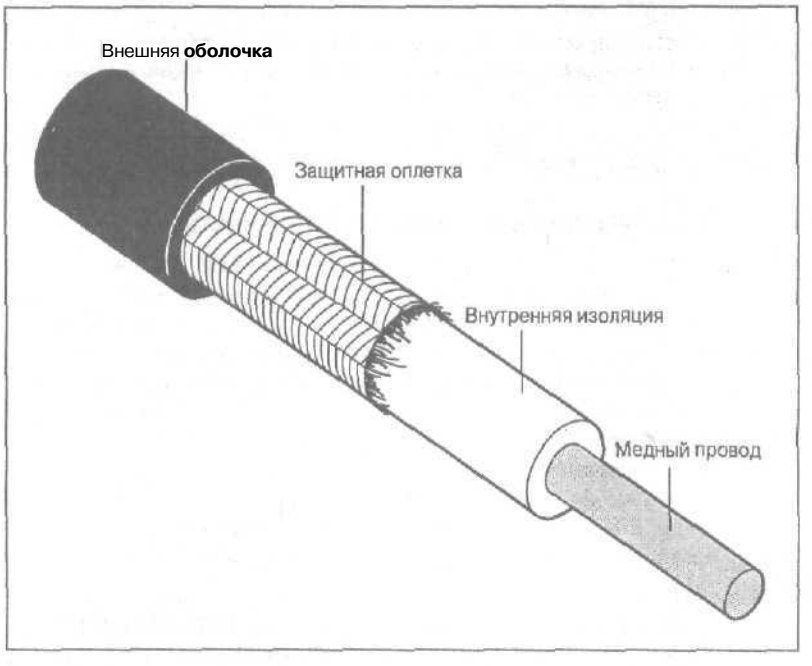


Рис. 7.2. Поперечный разрез коаксиального кабеля

Таблица 7.1. Классификация коаксиальных кабелей

Тип кабеля	Наименование	Волновое сопротивление (Ом)	Использование
RG-8 и RG-11	ThickNet	50	Сети Thick Ethernet
RG-58	ThinNet	50	Сети Thin Ethernet
RG-59	Широкополосный	75	Кабельное телевидение
RG-62	ARCnet	93	Сети ARCnet

При выборе любой версии кабеля RG-58 для сети убедитесь в том, что вы выбираете одну из многочисленных его разновидностей, обладающих плетеным сердечником (либо RG-58A/U, либо RG-58C/U). Хотя существует вариант со сплошным сердечником, который называется RG-58/U, он не охватывается спецификацией IEEE для сети 10Base2, и его использование в этой сети может иногда вызывать проблемы.

Вы, вероятно, заметили, что в табл. 7.1 мы ввели некоторые новые термины — ThickNet и ThinNet. Это просто другая классификация коаксиальных кабелей для сетей Ethernet. Мы опишем их более подробно в следующем разделе, поскольку они зачастую применяются в небольших организациях.

Что вам следует знать о сетевых транках

Транк, или ***транковое соединение*** (trunk), — это сетевой сегмент, состоящий из целостного кабельного сегмента, который идет от одного повторяющегося устройства-повторителя к другому, к которому может быть подключен (или не подключен) отдельный компьютер. Для сети 10Base2 транк может иметь длину до 185 метров, и к нему можно подключить не больше 30 устройств. Каждое устройство транка сети 10Base2 должно отстоять от следующего устройства как минимум на 50 сантиметров.

Вы не можете использовать отдельный цельный кабельный сегмент длиной больше 91,5 метра. Это означает, что сегмент, который простирается на 185 метров, должен содержать по меньшей мере три устройства. Если вы проигнорируете это ограничение, ваша сеть, вероятно, будет испытывать трудности. Вы можете, однако, добавить к сетевым транкам устройства-повторители, увеличив, таким образом, длину вашей сети.

Устройства-повторители принимают входящие сигналы из сети, снимают шумы, усиливают сигнал и передают данные следующему сегменту сети. Однако, что касается сети 10Base2, даже если вы используете повторители, ее максимальная протяженность имеет физические ограничения. Общая протяженность сети не может превышать 925 метров, и вы не можете (теоретически) разместить больше 1024 устройств в рамках одной объединенной сети 10Base2 вдоль всех кабельных сегментов (на практике, как показали эксперименты, фактический предел составляет 900 устройств).

Стоимость коаксиального кабеля прямо пропорциональна его диаметру. Чем больше диаметр, тем дороже кабель; не случайно, что и соответствующее оборудование также стоит дороже.

10Base2 (ThinNet)

Для сети *ThinNet* существует несколько альтернативных названий, таких RG-58, CheaperNet, ThinWire и 10Base2. Запомните, что сеть 10Base2 означает использование кабеля, рассчитанного на скорость передачи данных 10Мбит/с, а ее общая протяженность не превышает 185 метров (хорошо, что ее обозначение не выглядит как 10Base1.85) без использования каких-либо повторителей. Это самый тонкий тип коаксиального кабеля (отсюда и названия ThinWire ("Тонкий

провод"), ThinNet ("Тонкая сеть")), который пользуется большой популярностью из-за своей дешевизны (отсюда пошло название CheaperNet ("Более дешевая сеть")).

Сеть ThinNet отличается гибкостью и легкостью в работе, поскольку она довольна "тонкая". Сети типа ThinNet можно встретить в небольших организациях, офисы которых занимают всего один этаж или одно помещение, поскольку они дешевле сетей на основе кабелей UTP категории CAT 5 и STP и не требуют специально выделенных устройств связи, таких как концентраторы.

Поскольку кабель 10Base2 тоньше, чем кабель UTP, он требует использования коннекторов забавной формы, которые вы, вероятно, видели в радиокабинке, но не узнали. Эти коннекторы называются *BNC-коннекторами* (British Naval Connector — британский морской коннектор) или *Т-коннекторами*. Последнее название коннектора описывает его форму — в виде буквы Т. Верхняя часть Т-коннектора соединяет кабельные сегменты, а к нижней части подключается кабель, ведущий к адаптеру компьютера. Кроме того, для сети на основе кабеля 10Base2 требуется терминальный согласующий резистор на каждом конце каждого кабельного сегмента, один из концов которого зачастую заземлен.

Итак, как вы должны подключать компьютеры и устройства к сети с использованием кабеля 10Base2? Сначала нарисуйте прямую линию с подключенными к ней устройствами. Сеть 10Base2 относится к шинной топологии (см. главу 4), так что она протягивается в виде прямой линии, где каждое сетевое устройство подключается между двумя кабельными сегментами. Устройства подключаются к сети через нижнюю часть Т-коннектора, которая вставляется в адаптер с тыльной стороны каждого компьютера.

На неиспользуемых концах Т-коннектора с каждой стороны сетевого сегмента сети 10Base2 следует установить резисторы-терминаторы.

При установке сети 10Base2 следите за количеством устройств, которые поддерживают отдельные кабельные сегменты, и длиной подобных кабельных сегментов. В табл. 7.2 представлена ключевая информация, с которой вам необходимо ознакомиться до того, как вы приступите к установке сети 10Base2 или проверке существующей сети.

Таблица 7.2. Ограничения сетей 10Base2

Характеристика	Транковый сегмент соединения	Вся сеть
Максимальная длина	185м	925 м
Максимальное количество узлов	30	1024
Минимальное расстояние между узлами	50 см	50 см
Максимальное количество повторителей	Информация отсутствует	4
Максимальное количество сегментов	Информация отсутствует	5

10Base5 (ThickNet)

10Base5, или ThickNet ("Толстая сеть"), представляет собой более толстый и, как следствие, более дорогой, чем 10Base2, коаксиальный кабель. Он также менее гибкий и подчиняется более жестким ограничениям в отношении радиуса изгиба. (На обыденном языке это означает, что если вы резко изогнете кабель, он перестанет нормально работать.) Если вы можете себе отчетливо представить попытку проткнуть небольшую дырочку в замерзшем садовом шланге, вы быстро поймете, что вам необходимо специальное зажимное или прокалывающее устройство, чтобы справиться с толстыми внешними оболочками.

Чтобы подключить сетевые устройства к коаксиальному кабелю 10Base5, вам необходимо специальное устройство — *пронзающий ответвитель,* или "зуб вампира" *(vampire tap),* — вместо Т-коннекторов, которые используются с кабелем 10Base2. Ответвитель вводится в коаксиальный кабель и проникает сквозь оболочку до его внутреннего проводника. Для преобразования цифровых сигналов компьютера в электрические сигналы в проводнике (*и* наоборот) вам необходимо использовать трансивер.

Рабочая станция подключается к кабелю 10Base5 с помощью внешнего трансивера и может поддерживать кабели трансиверов длиной до 15 метров, что позволяет кабелю 10Base5 выполнять функции своего рода магистрали, а кабелям трансиверов — удлинять расстояние от кабеля 10Base5 до настольных машин. Это несколько облегчает прокладку "замерзшего садового шланга", поскольку он не должен извиваться от компьютера к компьютеру, как в случае кабеля 10Base2.

Типичная схема размещения кабеля 10Base5 показана на рис. 7.3. Подобный монтаж также объясняет, почему кабели 10Base5 используются преимущественно для сетевых магистралей либо в старых сетях, которые не изменялись с момента их первоначальной установки (с 1970-х - начала 1980-х годов, когда этот кабель представлял собой единственно доступную технологию Ethernet).

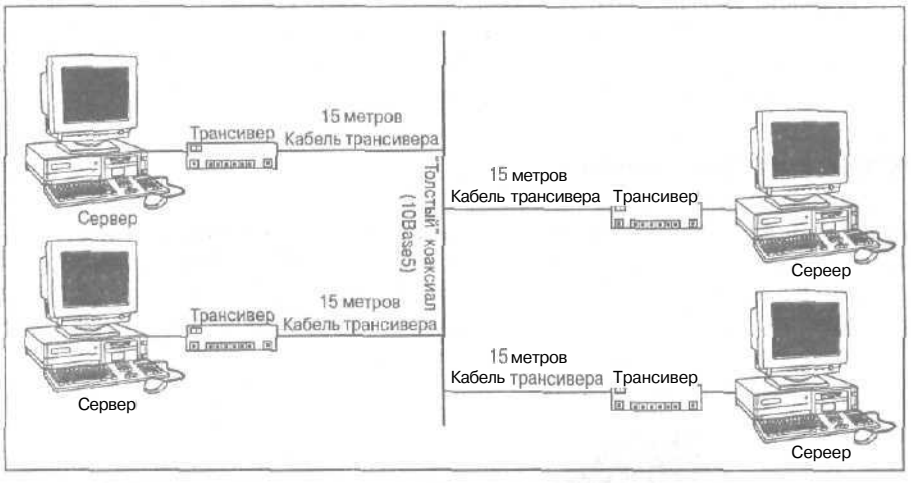


Рис. 7.3. Кабели трансивера сети 10Base5 могут иметь протяженность до 15 метров

В табл. 7.3 приведены ограничения на расстояния и количество узлов в сетях на базе кабеля 10Base5.

Таблица 7.3. Ограничения сетей 10Base5

Характеристика	Транковый сегмент	Сеть в целом
Максимальная длина	500 м	2500 м
Максимальное количество узлов	100	1024
Минимальное расстояние между узлами	2,5 м	2,5 м
Максимальное количество повторителей	Информация отсутствует	4
Максимальное количество сегментов	Информация отсутствует	5

Хотя сеть 10Base5 допускает объединение до 5 сегментов, интересно отметить, что только три из этих кабелей могут содержать сетевые устройства. Это ограничение известно в сети Ethernet как "правило 5-4-3": на любом маршруте в сети от одного терминатора до другого до пяти кабельных сегментов могут быть объединены с помощью не более чем четырех повторителей, но только три из этих кабельных сегментов могут быть нагружены более чем двумя устройствами.

Если ваша сеть невелика, а бюджет ограничен, коаксиал может быть неплохим решением, однако благодаря фактору стоимости и легкости установки сеть на основе "тонкого коаксиала" — ThinWire — всегда будет лучшим вариантом для подобных систем, чем "толстый коаксиал" (ThickWire). Однако если ограничения на длину кабеля для ThinWire не позволяют вам добиться необходимой протяженности сети, вы можете совместить эти два типа кабеля.

Для ускорения установки сети вы можете приобрести сборные кабели различной длины. В противном случае вам придется купить специальный обжимной инструмент и компоновать подобные кабели самостоятельно. Если вы решили заняться сборкой сами, потратьте дополнительно 200 долларов и купите недорогой тестер кабеля, чтобы ваши кабели были соединены надлежащим образом. На Web-узле компании Microtest (www.microtest.com) — наиболее известного сегодня поставщика кабельного оборудования — вы можете больше узнать о таких инструментах, как кабельные дефектоскопы, измерители коэффициента отражения и обжимные инструменты, и ознакомиться с соответствующей документацией и спецификациями на кабельную продукцию.

Волоконно-оптические кабели

Волоконно-оптический кабель отличается от витой пары и коаксиального кабеля, поскольку он передает данные с помощью световых сигналов, а не электрических импульсов. Если вы посмотрите, как устроен этот кабель, то вам покажется, что он похож на коаксиал, но в нем в качестве внутреннего проводника вместо меди используется пластмассовое или стекловолокно. На рис. 7.4 показано, как выглядит волоконно-оптический кабель в разрезе.

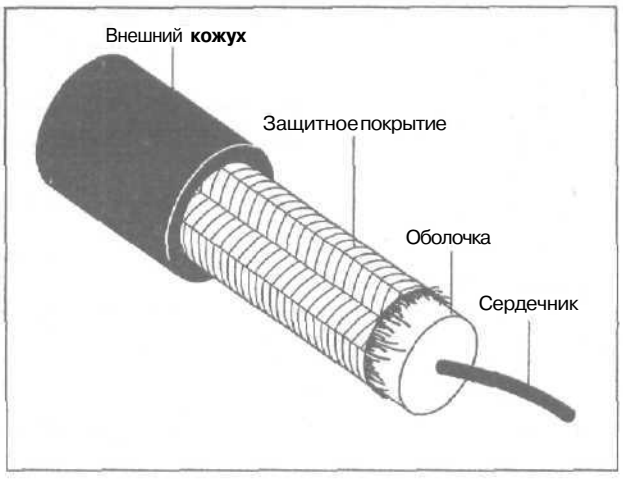


Рис. 7.4. Волоконно-оптический кабель в разрезе

Обратите внимание, что внутренний стеклянный сердечник (см. рис. 7.4) иногда называется защитным покрытием и что весь кабель покрыт еще одной жесткой оболочкой. Внешняя оболочка достаточно толстая, чтобы защитить внутреннее волокно от разрыва при обращении с кабелем.

Хотя волоконно-оптический кабель дороже электрических кабелей, он отличается большей пропускной способностью; это означает, что он может передавать большие объемы данных на большие расстояния. Волоконно-оптический кабель невосприимчив к электромагнитным помехам и другим источникам шумов, которые оказывают воздействие на электропроводящие кабели. Дороговизна волоконно-оптического кабеля также обусловлена необходимостью проявлять крайнюю осторожность при его установке. Знающий специалист должен тщательно отполировать каждое стекловолокно с помощью специальных инструментов, а затем добавить к кабелю специальные разъемы.

Волоконно-оптические кабели зачастую прокладывают между зданиями в кампусах или между этажами внутри зданий. Из-за дороговизны вы редко встретите этот тип кабеля, протянутого к настольным системам, — вы должны использовать специальный адаптер, и, кроме того, к каждой рабочей станции должны быть подключены два кабеля, поскольку один кабель передает исходящие сигналы, а второй получает входящие. Хотя "аппетиты" в отношении пропускной способности постоянно растут, не рассчитывайте, что ваш настольный компьютер в обозримом будущем сядет на богатую волокном диету!

В некоторых местах, таких как клиники, к определенным настольным компьютерам необходимо подводить волоконно-оптические кабели, поскольку рентгеновские лучи и оборудование, а также магнитно-резонансные томографы могут создавать помехи в электрических кабелях. Кроме того, требования медицинского оборудования к пропускной способности для интроскопии настолько высоки, что обычные электрические кабели не могут справиться с соответствующим трафиком.

Чтобы световой сигнал проходил по волоконно-оптическому кабелю, к одному его концу должен быть подключен передатчик, а к другому — приемник. Вот почему, чтобы дать возможность любому устройству отправлять и получать сигналы, необходимы два кабеля. На передающем конце инжекционный лазерный диод (injection laser diode — ILD) или светоизлучающий диод (light-emitting diode — LED) посылает световые импульсы по кабелю. Эти световые импульсы передаются внутри стеклянной сердцевины и отражаются от подобной зеркалу оболочки на всем протяжении кабеля, пока не достигнут фотодиодного приемника на другом конце кабеля. Обратите внимание на то, что данные перемещаются только в одном направлении. Приемник преобразует входящие световые импульсы в электрические сигналы и передает данные сетевому адаптеру.

Способ, с помощью которого световые импульсы движутся по волоконно-оптическому кабелю, требует особой тщательности при сращивании двух таких кабелей, чтобы не снизить способность кабеля проводить сигналы. В противном случае световой импульс может достичь места соединения, но не пройти через него к другому концу кабеля. Мы называем подобную ситуацию *плохим сращиванием,* но ваши пользователи станут называть ее значительно хуже!

Волоконно-оптический кабель — наиболее дорогостоящий тип кабеля, однако он обеспечивает самую высокую пропускную способность и наибольший резерв для ее нарашивания в будущем.

Заключительные замечания по поводу кабельных систем

Если вы принялись за установку кабеля сами, а не наняли для этого подрядчика, мы хотели бы поделиться с вами некоторыми заключительными замечаниями на эту тему.

- ✓ **Добудьте копию чертежей вашего здания или этажа и позаботьтесь о том, чтобы на них были четко обозначены все электрические устройства и розетки.** Подобная схема поможет вам размесить кабель вдали от электрических устройств или моторов, которые могут создавать помехи в сети. Не прокладывайте кабель вблизи лифтовых моторов, трансформаторов и других мощных электрических устройств (если только вы не используете волоконно-оптический кабель, но даже в этом случае вы должны защитить его от потенциальных источников повреждений и износа).
- ✓ **Внимательно ознакомьтесь с местными, региональными и государственными строительными нормами и правилами и убедитесь в том что, ваши планы соответствуют их положениям.** Вам необходимо оценить эти требования до того, как вы приобретете какой-либо кабель, поскольку некоторые нормы требуют приобретения огнестойких *усиленных* (*plenum-rated*) кабелей со специальной тефлоновой оболочкой, рассчитанных на прокладку внутри стен, в вентиляционных каналах и т.д. Некоторые нормы требуют использования усиленных кабелей, но только в тех случаях, когда существует опасность их быстрого загорания. Как бы там ни было, вам надлежит знать эти нормы до приобретения оборудования и установки сети.

Пленум (plenum) — вентиляционный канал между потолком одного этажа и полом другого этажа, в котором зачастую протягивается кабель. В этих полостях огонь распространяется очень быстро за счет быстрого переноса движущимся воздухом; поэтому усиленные кабели обязательны для использования в подобном пространстве, чтобы воспрепятствовать распространению огня и дыма в здании.

- ✓ **Определите, какие части сети вы можете создать и поддерживать самостоятельно, а какие требуют заключения договора с субподрядчиком.** Например, если у вас есть время и желание прокладывать кабели, а также есть время на поиск и устранение неисправностей в сети, когда эти кабели не работают, пожалуйста,- занимайтесь этим. Мы рекомендуем вам приобрести как можно больше сборных кабелей и готовить кабели самостоятельно только в том случае, если у вас нет другого выхода. Почему? Потому что компании, которые изготовляют кабели, занимаются этим постоянно и достигли в этом мастерства. Если вы готовите кабели для вашей сети только от случая к случаю, вы можете привнести проблемы.
- ✓ **Старайтесь нанять специалистов для установки кабелей ЛС.** Проводка — инфраструктура вашей сети. Если проводка установлена не надлежащим образом, она может привести к бесконечному хаосу в сети. Фирма, специализирующаяся на установке кабельных систем, обеспечит вас заявкой на подряд, проложит кабели, проведет испытание и сертификацию всех кабелей и обеспечит вас итоговой документацией. Вы отвечаете за то, чтобы проследить за всем этим. Не думайте, что подрядчик станет следовать частным предписаниям, пока вы не заставите его сделать это. Фиксируйте все ваши предположения в письменном виде и следите за работой.

Увеличение потолка пропускной способности

По мере того как организации все более полагаются в своей деятельности на локальные и глобальные сети, они размещают в них все больше приложений и информации. Быстрый доступ к такой информации становится для подобных организаций критически важным фактором их успешной деятельности, а иногда — и выживания. Быстрый доступ — это именно то место, где необходимость в дополнительной пропускной способности наиболее часто заявляет о себе.

Традиционные чисто текстовые документы обычно не слишком нагружают сеть. Но сегодня данные зачастую принимают звуковую, визуальную или графическую форму и представляют другие типы мультимедиа. Подобные файлы или потоки данных значительно превосходят по объему простые текстовые файлы и зачастую накладывают ограничения на сеть по предельному времени доставки данных. Если вам трудно понять, как это выглядит на деле, представьте себе, какую досаду вызывает рассогласование звукового и видеоряда вашего телевизора, а затем умножьте эту досаду в десятки раз. А теперь представьте себе, что в действительности требуется для своевременной доставки аудио, видео и мультимедиа по сети.

Подобные сложные формы данных легко могут поглотить всю пропускную способность обычной 10-мегабитовой сети, чтобы справиться с запросами всего одного или двух пользователей. Вот почему так стремительно растут "аппетиты" на каждом рабочем месте в отношении сетей с более высокой пропускной способностью. Потребность в дополнительной пропускной способности возрастает в связи с необходимостью обработки более сложных типов данных, перемещающихся по сети, и подготовки инфраструктуры для работы с вновь появляющимися приложениями наподобие сетевых телеконференций, сетевой телефонии, кооперативной работы над проектами и многих других видов невероятных технологий, которые находятся сегодня в стадии разработки.

Вот почему мы чувствуем себя обязанными рассказать о некоторых альтернативных вариантах кабельных систем, выпускаемых для сетей, которые, вероятно, способны в ближайшем будущем справиться с возрастающими потребностями в пропускной способности. Если вы действительно стремитесь понять больше, пожалуйста, ознакомьтесь с врезками, приведенными в этой главе.

100-мегабитовая Ethernet

На сегодняшний день существуют две разновидности сетей Ethernet с пропускной способностью 100 Мбит/с, каждая из которых обладает собственным методом доступа: CSMA/CD (Carrier Sense Multiple Access with Collision Avoidance — множественный доступ с контролем несущей и предотвращением конфликтов; см. главу 4) и приоритетный доступ по запросу (описывается ниже в этой главе). Когда были затребованы предложения, касающиеся 100-мегабитовой Ethernet, появились две группировки: одна использовала тот же самый метод доступа CSMA/CD, применяемый в традиционной технологии Ethernet (ее предложения теперь известны как сеть Fast Ethernet или 100BaseT), а другая использовала приоритетный метод доступа по запросу (теперь они известны как сеть 100BaseVG-AnyLAN).

Обе группировки предложили реализовать свои подходы. Забавно, что оба предложения были безоговорочно приняты как стандарты, но каждое из них попало в сферу действия разных комитетов ШЕЕ. Сегодня стандарт Fast Ethernet входит в семейство стандартов ШЕЕ 802.3, а стандарт 100BaseVG-AnyLAN — в семейство стандартов ШЕЕ 802.12.

Стандарт 100BaseT аналогичен lOBaseT за исключением того, что он работает в 10 раз быстрее. При внедрении стандарта 100BaseT необходимо использовать оборудование, спроектированное для сетей 100BaseT, а в остальном проектирование и создание сети мало чем отличается от сети стандарта lOBaseT. Технологии lOBaseT и 100BaseT можно даже сочетать в рамках одной сети, но чтобы соединить эти два мира, вам необходимо включить в состав сети концентраторы с возможностями поддержки передачи данных как со скоростью 10 Мбит/с, так и со скоростью 100 Мбит/с.

Стандарт 100BaseVG-AnyLAN рассчитан на такую же пропускную способность, что и стандарт 100BaseT, но использует в каждом кабеле четыре пары проводников вместо двух. Удвоение количества пар проводников позволяет применить для управления доступом к сетевой среде другой метод доступа, называемый *приоритетом по запросу (demand priority)*. Кроме того, технология 100BaseVG-AnyLAN позволяет сетевым устройствам осуществлять одновременный прием и передачу данных (это одна из причин, по которой количество пар проводников в кабеле удвоено).

Концентраторы 100BaseVG-AnyLAN помогают управлять схемой приоритетов по запросам и обеспечивают службу арбитража в тех случаях, когда несколько запросов на доступ к сети появляется примерно в одно и то же время. При использовании метода доступа CSMA/CD рабочие станции, прежде чем отправить сообщение, прослушивают сетевую среду, и как только они устанавливают, что сетевая среда не используется, осуществляют передачу. Подобный порядок приводит к коллизиям, когда две или более станций начинают пересылку сообщений практически одновременно, в особенности по мере возрастания уровня использования сети. Когда устройство, работающее по методу приоритетного доступа по запросу, пытается передавать данные по сети, оно подает сигнал концентратору, и концентратор определяет, когда это устройство может осуществить доступ к сети. Такая схема исключает коллизии и позволяет сетям функционировать с более высокой эффективностью, чем в состоянии обеспечить метод доступа CSMA/CD.

Отрицательной стороной стандарта lOOBaseVG-AnyLAN является то, что сетевое оборудование и кабели, соответствующие стандарту 100BaseVG-AnyLAN, обходятся значительно дороже, чем для сети 100BaseT, даже с учетом более высокой производительности сетей lOOBaseVG-AnyLAN. Возможно, именно поэтому сети 100BaseT получили более широкое распространение на рынке, чем сети lOOBaseVG-AnyLAN.

Технология Gigabit Ethernet

Возможно, вы удивитесь тому, что вы можете сотворить с вашей сетью, когда возможности ее пропускной способности станут иссякать, даже с учетом использования технологии, обеспечивающей скорости передачи данных 100 Мбит/с. Речь идет о о дальнейшем развитии высокоскоростных сетей — технологии Gigabit Ethernet. Хотя технология Gigabit Ethernet сегодня доступна, она еще не получила широкого распространения. Однако поскольку потребность в скорости никогда не уменьшится, мы хотели бы дать вам "вкусить" этой технологии, чтобы у вас, как говорится, "слюнки потекли", — пусть даже она в ближайшее время и не появится в вашем офисе.

Надо сказать, что технология Gigabit Ethernet обычно не используется в качестве сетевого решения для настольных систем. (В действительности ни один обычный ПК или другая настольная машина не в состоянии "насытить" сеть Gigabit Ethernet.) Технология Gigabit Ethernet скорее используется в основном как базовая, в особенности в больших сетях, где на определенные магистрали приходится трафик большого объема. В идеальном случае технология Gigabit Ethernet помогает усилить взаимодействие серверов и позволяет передавать данные со сверхвысокими скоростями между коммутаторами сетевой магистрали.

Технология Gigabit Ethernet использует метод доступа CSMA/CD, а также размер кадра и форматы, аналогичные обычной технологии Ethernet. Поэтому вы легко можете интегрировать эту технологию в существующие сети Ethernet, и вам нет необходимости приобретать новые анализаторы протоколов, ПО управления сетью и т.п.

Чтобы влиться в ряды сторонников Gigabit Ethernet, вам необходимо добавить в сеть следующие устройства.

- ✓ Подходящие сетевые адаптеры и разъемы для серверов.
- ✓ Соответствующие кабели (в большинстве случаев — волоконно-оптические, хотя в стадии разработки находится вариант с витой парой).
- ✓ Обновить маршрутизаторы и коммутаторы, которые управляются с трафиком Gigabit Ethernet.

В некоторых случаях этот находящийся в стадии становления стандарт может потребовать от вас заменить определенные компоненты оборудования; заметим, однако, что современные маршрутизаторы и коммутаторы требуют только новых микросхем EPROM (Erasable Programmable Read-only Memory — стираемое программируемое постоянное запоминающее устройство) и обновления для некоторых плат сетевого интерфейса. Со временем, по мере снижения цены технологии, вы можете даже рассмотреть возможность добавления интерфейсов Gigabit Ethernet к вашим высокопроизводительным рабочим станциям. Однако в ближайшие несколько лет необходимость в этом вряд ли возникнет.

Альянс разработчиков Gigabit Ethernet (Gigabit Ethernet Alliance) предлагает отличный документ, посвященный этой технологии. Вы можете загрузить его с Web-узла www.10gea.org/ (загляните в технологический раздел этого Web-узла, включающий документ 10GEA). Он дает великолепный обзор технологии Gigabit Ethernet и описывает типы приложений, которые требуют подобных сетевых скоростей.

Магистраль подключена ко... всему остальному!

Как уже говорилось в этой главе, технологии 10Base5 и Gigabit Ethernet одинаково хорошо подходят для сетевых магистралей. Если в сети имеются главные магистрали, почему бы ей не содержать "боковых" и "хвостовых" магистралей?

В сетевых технологиях *магистраль (backbone)* — это определенный кабельный сегмент, который соединяет другие кабельные сегменты или обеспечивает высокоскоростной канал, аккумулирующий большие информационные потоки, для распределения высокоуровневого сетевого трафика по кабельным сегментам. Если вы на минутку призадумаетесь над этой ситуацией и взглянете на рис. 7.5, то начнете понимать, что выражения "кабельный сегмент, который соединяет другие кабельные сегменты" и "кабельный сегмент, аккумулирующий большие информационные потоки" — это два способа выразить одно и то же понятие.

Попросту говоря, магистраль обеспечивает канал, объединяющий в одно целое множество кабелей. Соответственно тому, как растут запросы отдельных пользователей к пропускной способности сети, увеличивается и трафик, который должна передавать магистраль. Магистрали также зачастую обеспечивают связь с внешними ресурсами, такими как Internet, или доступ к огромным централизованным совокупностям данных, таким как базы данных мэйнфреймов и др.

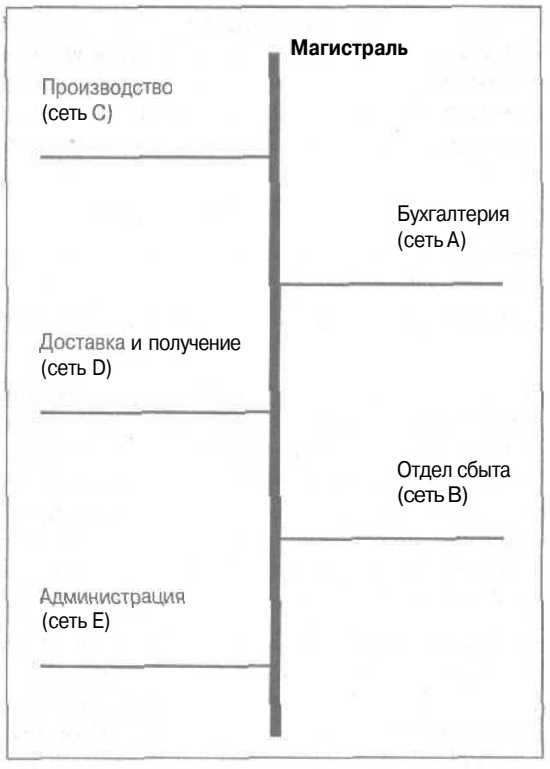


Рис. 7.5. Магистраль ***соединяет в одно*** *целое все фрагменты сети*

Больше одной сети — это объединенная сеть

Еще одна **тонкость** создания **сетей связана с взаимоотношениями** между отдельными **кабельными сегментами и сетью,** которая **их содержит.** В силу **исторических причин,** которые **слишком** долго **объяснять, термин *сеть (network)* зачастую применяется для описания только тех устройств, которые присоединены к одному кабельному сегменту.**

Все разнообразие глобальных каналов связи

Глобальные каналы связи представляют широкий спектр функциональных возможностей, значений пропускной способности и соответствующей стоимости и включают целый ряд технологий. Система Windows Server 2003 делает доброе дело, поддерживая все типы глобальных каналов, поскольку является многопротокольной и включает возможности по маршрутизации.

- ✓ **ISDN (Integrated Services Digital Network — цифровая сеть с комплексными услугами).** Этот сравнительно низкоскоростной канал связи осуществляет соединение посредством телефонных систем, придавая им поистине глобальный размах. Сервер Windows Server 2003 включает встроенные драйверы

Г

для различных интерфейсов и поддерживает широкий спектр значений пропускной способности. Обычно ISDN-соединение осуществляется посредством так называемого интерфейса базового уровня (basic rate interface — BRI) и поддерживает один или два канала передачи данных на скорости 64 Кбит/с для максимальной пропускной способности 128 Кбит/с. Ежемесячная плата за типичное ISDN-соединение варьируется от 100 до 500 долларов. Для некоторых каналов ISDN плата за использование накапливается поминутно, так что не забудьте проверять свою местную телефонную компанию.

- **xDSL-линии (Digital** Subscriber **line** - цифровая абонентская линия). Этот термин описывает технологию с высокой пропускной способностью, которая также использует обычные телефонные линии для обработки цифровых данных. (Существует несколько типов DSL-линий, поэтому символ x обозначает "общие".) Система Windows Server 2003 включает драйверы для целого ряда xDSL-устройств. Наиболее распространенные xDSL-устройства обеспечивают пропускную способность в диапазоне от 256 Кбит/с до 1,544 Мбит/с. Стоимость использования xDSL-линий на многих рынках остается неясным вопросом, однако все, кажется, идет к тому, что xDSL-линии полностью заменят линии ISDN.
- ✓ Кабельные модемы, Кабельные модемы для отправки и получения сетевых данных используют коаксиальные кабели абонентского телевидения. Хотя кабельные модели доступны не на всех рынках, большинство центральных районов, обслуживаемых такими национальными телевизионными компаниями, как Time Warner и Cox Communications, предлагают соединения с использованием кабельных модемов. Кабельные модемы, как правило, обеспечивают высокую прямую пропускную способность (до 1,544 Мбит/с для входящих данных) и более низкую обратную пропускную способность (до 512 Кбит/с для исходящих данных). Кабельные модемы намного дешевле и могут обходиться до 40 долларов s месяц (однако, в отличие от всех упомянутых выше альтернатив, среда является разделяемой, поэтому отдельным пользователям достается меньше "пропускной способности").
- ✓ **Спутниковые** каналы. Некоторые поставщики услуг спутникового телевидения начали предлагать высокоскоростной спутниковый доступ к Internet & большинстве случаев скорость загрузки превосходит скорость выгрузки всего лишь в 2–10 раз, но если у вас нет возможности подключить сеть к поставщику услуг Internet или телекоммуникационной системе, этим способом стоит воспользоваться. Большинство спутниковых каналов связи обходятся от 50 до 500 долларов в месяц.
- ✓ Соединения **T1/E1** и **T3/E3.** Эти термины обозначают наиболее распространенные высококачественные цифровые службы для средних и крупных компаний. Службы T1/T3 представляют два класса цифровых служб, используемых в Северной Америке; E1/E3 — службы аналогичного класса, нашедшие распространение в Европе и на других континентах. Пропускная способность службы T1 равна 1,544 Мбит/с; для T3 — 45 Мбит/с; для E1 — 2,048 Мбит/с; для E3 — 34,368 Мбит/с. Использование всех этих служб обходится не меньше 500 долларов в месяц, кроме того, для них необходимо дорогостоящее оборудование. На большинстве рынков стоимость служб T3/E3 доходит до 20000 долларов в месяц.
- ATM **(asynchronous** transfer mode - асинхронный режим передачи). Этот термин описывает в высшей степени высокоскоростную технологию. Эта технология глобальных сетей подходит телефонным и другим телекоммуникационным компаниям, отличается большим разнообразием вариантов реализации, которые обеспечивают скорость передачи данных от 155 Мбит/с до 2,48 Гбит/с. Система Windows Server 2003 включает поддержку различных реализаций стандарта ATM.

Подобная ограниченная интерпретация слова *сеть* (*network*) требует введения понятия *объединенная сеть* (*internetwork*). Объединенная сеть появляется там, где несколько устройств (таких как повторители, мосты, маршрутизаторы и шлюзы) подключается к двум или более кабельным сегментам для создания сети сетей. В объединенных сетях информация из одного кабельного сегмента может проходить через одно или несколько этих устройств для перемещения из одного кабельного сегмента в другой. "Предком" всех объединенных сетей является Internet, которая представляет собой сеть такого большого количества сетей, что это трудно вообразить.

Когда вы участвуете в разговоре на сетевую тему, убедитесь в том, что вы верно истолковываете значение слова *сеть в* контексте ведущегося обсуждения. В большинстве случаев не важно, что в действительности то, о чем упоминают как о сети, является объединенной сетью, но когда это имеет значение, это крайне важно. Будьте внимательны!

За пределами локальных сетей

Раз разговор о магистралях привел нас к Internet, разговор на тему об объединенных сетях непременно приведет к размышлениям о глобальных сетях. В прежние времена только компании-"толстосумы" могли позволить себе связь на уровне глобальной сети. Сегодня, когда ISP-соединения (Internet Service Provider — поставщик услуг Internet) с высокой пропускной способностью используются интенсивнее, небольшие и средние фирмы должны побеспокоиться об установлении межсетевого обмена между своими и другими сетями с использованием разнообразных протяженных цифровых каналов.

Все, что требуется от вас для установления межсетевого обмена для большинства сетей на базе сервера Windows Server 2003, — знать, как подключиться к местному поставщику услуг Internet. В большинстве случаев требуется технология T1 или более медленные технологии. В подобных ситуациях система Windows Server 2003 надежно работает как маршрутизатор или же отлично работает с внешними устройствами маршрутизации, чтобы помочь вам установить внешнее соединение, необходимое для сети.

Часть III

Серверы, запустить моторы!

"Я не могу сказать, что верю во всякую чепуху. Но я знаю, что с тех пор, как он здесь, наш сервер работает вдвое быстрее".

В этой части...

После знакомства с основами создания сетей вы можете ознакомиться р. подробностями, связанными с установкой и настройкой конфигурации Windows Server 2003. Именно этим вопросам посвящена данная часть. Сначала в ней описывается семейство продуктов Windows 2003 (это нечто большее, чем простой сервер) и подробно рассматриваются вопросы установки и настройки конфигурации ПО Windows Server 2003, Затем рассматриваются связь сервера Windows Server 2003 с внешним миром, а также способы коммутируемого доступа к вашим пользователям.

После этого настанет черед перейти к Active Directory — "нервному центру" Windows Server 2003. Установке, настройке конфигурации и использованию этой мощной функции Windows .2000 и семейства Server 2003 посвящены две закрепляющие главы. Затем будет описана работа с принтерами и службами печати в среде Windows 2003. Эта часть завершается обсуждением системы адресации протоколов TCP/IP и описанием подробностей конфигурирования, которые наверняка заинтересуют всех, кто работает с Windows Server 2003, либо просто дослужат источником полезной информации.

Короче "говоря, в части III описаны все шаги, необходимые для того, чтобы установить систему Windows Server 2003 и сделать ее полезной для ваших пользователей. Хотя некоторые ее более экзотические и, необычные службы не рассматриваются в этой части, материал, включенный в нее, выведет вашу сеть на штатный режим и поможет ей работать "без шума и пыли".

По ходу дела вы поймете, как создать мощную сетевую среду, опираясь на Windows Server 2003, включая настройку конфигурации базовой системы, настройку конфигурации сети, сетевые службы и службы каталогов. Вы также узнаете, как использовать Windows Server 2003 для доставки по сети всякой всячины, будь то данные для файловой службы, или службы печати, или нечто более захватывающее.

Глава 8

Знакомимся с Windows 2003

В этой главе...

- Преемница системы Windows 2000
- Основы Windows 2003
- Оценка преимуществ, которые может дать Windows 2003

Windows Server 2003 — часть нового мировоззрения компании Microsoft, направленного на создание инфраструктуры, которую могут использовать компании, чтобы быстро и эффективно предоставить в распоряжение клиентов богатые возможности Web-приложений электронной коммерции. Другими словами, Microsoft стремится поощрить многие компании к использованию ее продуктов для создания интерактивных торговых пассажей. Чтобы внести в дело свежую струю, компания Microsoft добавила в свои технологии разработки и развертывания Web-приложений некоторые усовершенствования.

Однако нам кажется, что это очень похоже на попытку пустить пыль в глаза. По мере того как вы станете осваивать Windows Server 2003 самостоятельно и с помощью этой книги, вы обнаружите небольшие различия между Windows Server 2003 и ее предшественницей — Windows 2000 Server. Конечно, исправлены некоторые ошибки, усовершенствованы функции, введены более жесткие правила безопасности, используемые по умолчанию. Однако сервер Windows Server 2003 может входить в состав доменов Windows 2000; он даже может без проблем служить в качестве контроллера домена. Все пользовательские элементы управления и средства администрирования также остались прежними.

Итак, что же вы приобретете с Windows Server 2003? Вы приобретете более глубокий пользовательский опыт, который представляет собой небольшое смешение пользовательского интерфейса и рабочего стола Windows 2000 и Windows XP. Вы также получите несколько новых средств наподобие Remote Desktop, Remote Assistance, Microsoft .NET Framework Configuration и Microsoft .NET Framework Wizards. Два первых средства вы можете узнать по Windows XP, а два последних — нечто новое в мире Microsoft. Мы поговорим обо всех этих средствах в последующих главах.

Еще один момент: подобно Windows XP, Windows Server 2003 требует, чтобы вы активизировали вашу операционную систему в течение 30 дней после установки. Если этого не сделать, вы будете отключены — ОС запретит вам входить в систему и перестанет позволять делать все, что вам заблагорассудится. Активизация — еще одна головная боль для пользователей продуктов Microsoft; мы поговорим о ней в главе 9.

Основные сведения о Windows Sewer 2003

Система Windows Server 2003 построена на основе испытанной временем архитектуры Windows NT. Начиная с ранних версий серверных систем Windows NT, появившихся в начале 1990-х годов, первый серверный продукт — операционная система от Microsoft — прошел довольно долгий путь.

Сервер Windows Server 2003 предоставляет в распоряжение пользователей надежную и масштабируемую платформу для развертывания сложных внутрисетевых решений за счет интеграции Internet и возможностей локальной сети. Иначе говоря, этот продукт позволит вам играть в Doom с партнерами по офису или по всему миру.

Все возможности и преимущества, которыми вы пользовались, работая с сервером Windows **Server** 2000, по-прежнему присуши и серверу Windows Server 2003. Нам сложно придумать что-нибудь, чего бы вам недоставало (по меньшей мере, из того, чем вы действительно пользовались). Под слоем "косметики" легко можно обнаружить большую часть усовершенствований, введенных в Windows Server 2003. К последним, например, относятся способ работы Active Directory, расширение средств управления с использованием командной строки, усовершенствования в способе управления доменами, усиленные механизмы защиты, улучшенная служба Terminal Service, усовершенствование удаленного доступа (Remote Access) и службы Internet Information Services *(US).*

Невозможно не заметить изменений в интерфейсе окна Manage Your Server (Управление сервером), которое появляется автоматически при входе в систему. С помощью этого окна вы можете управлять ролями серверов и доступом к таким утилитам, как Administrative Tool, Windows Update, Help and Support Center и многим другим. По своему выбору вы можете использовать окно Manage Your Server или запускать утилиты и программы по-старому (с помощью кнопки Start (Пуск)). Чтобы пропустить окно Manage Your Server при входе в систему, установите в нижней части окна флажок Don't Display this Page at Logon (Не отображать эту страницу при входе в систему).

Платформа Windows 2003 от Microsoft в целом обещает некоторые интересные перспективы, которые сегодня могут стать реальностью. Наиболее важная из них — уменьшение усилий, требуемых для разработки и развертывания сложных Web-узлов электронной коммерции. Windows Server 2003 (так же как и остальная часть семейства ОС .NET) приспособлена к более эффективной работе с Internet и поддержке сетевых служб клиентов. При использовании Windows Server 2003 вместе с языками программирования и сетевыми службами Microsoft, ориентированными на технологию .NET, вы можете создать эффект весьма впечатляющего "интерактивного присутствия".

Семейство ftioiicriioe Windows 2003

Windows 2003 — не просто отдельный продукт, это семейство серверов и целая "куча родственников". Семейство Windows 2003 включает следующие четыре базовых представителя.

- **Windows** Server **2003, Web Edition,** Это новый тип сервера для Microsoft. Сервер оптимизирован для размещения Web-узлов и является единственным из серверов Windows Server 2003, который по умолчанию устанавливает службу IIS.
- **Windows Server** 2003, **Standard Edition.** Сервер одного уровня с сервером Windows 2000 — просто обычный сетевой сервер, с помощью которого можно создать домен и управлять им. Согласно определению Microsoft, "этот гибкий сервер — идеальный вариант для удовлетворения повседневных потребностей различных по своим масштабам фирм". Добавить тут, как говорится, больше нечего.
- **Windows Server 2003,** Enterprise **Edition.** Немного более надежная разновидность сервера. Он требует несколько большей вычислительной мощности, но может вернуть ее сторицей. Версия Enterprise Edition разработана для поддержки серверов инфраструктуры, что требует большей надежности и повышенной производительности.

- **Windows Server 2003, Datacenter Edition.** Это "дедушка" всех серверов от Microsoft. Он разработан с целью поддержки жизненно важных приложений, для которых требуется высокая отказоустойчивость, за счет использования масштабируемой кластерной архитектуры, которая отличается высокой степенью готовности. Иначе говоря, это могучий "зверь", с которым лучше не встречаться в поединке один на один.

Вы можете подумать: "Класс, что за роскошный ряд систем! Вряд ли можно найти что-то лучше!" Да, это именно то, к чему стремилась Microsoft. Чтобы расширить и распространить новую платформу Windows 2003, Microsoft заново позиционировала свои основные продукты в качестве серверов масштаба предприятия — *Enterprise Servers 2003. В* эту группу вошли следующие продукты,

- Семейство Windows 2000 Server (да-да, они по-новому разрекламировали свой старый продукт).
- Application Center 2000.
- BizTalk Server 2000.
- Commerce Server 2000.
- Content Management Server 2000
- Exchange Server 2000.
- Host Integration Server 2000.
- Internet Security and Acceleration Server 2000.
- Mobile Information 2001 Server.
- SharePoint Portal Server 2000.
- SQL Server 2000.

Если вы желаете получить источник, полный информации о семействе Windows 2003, посетите Web-узел `www.microsoft.com/net`. Все, что вам потребуется знать о новой платформе Windows 2003, просто-таки ждет не дождется вас здесь.

Почему Windows Server 2003?

Всякий раз, когда производитель объявляет о выходе новой версии (наподобие Windows 2003) популярного продукта, он должен создать побудительный мотив для пользователей предыдущих версий обновить их. Также компания должна привлечь к новой версии новых покупателей, чтобы поддержать рост продаж.

Что касается системы Windows Server 2003, то эти побудительные мотивы могут быть очень мощными. Системы Windows Server 2003 могут функционировать наряду с системами Windows 2000 Sewer как звенья домена или даже в качестве контроллеров домена. Windows Server 2003 также хорошо "играет" в одной команде со старыми версиями серверов Microsoft, такими как Windows NT Server, однако следует обратить внимание на заявление Microsoft о том, что Windows Server 2003 выступает во всем блеске, когда играет в команде с равными партнерами (иначе говоря, когда в сети присутствуют серверы только этого типа).

Более низкая стоимость владения

Общая стоимость владения (total cost of ownership — TCO) является мерой затрат на приобретение, установку, конфигурирование, управление и сопровождение системы на протяжении ее продуктивного жизненного цикла. В случае Windows Server 2003 мы имеем великолепный пример того, как Microsoft, "творя добро в силу необходимости", при конструиро-

вании этой системы приложила максимум усилий, чтобы снизить TCO. В результате получилось так, что многочисленные проблемы и дефекты, присущие Windows NT и Windows 2000, были устранены в Windows 2003.

Ниже перечислено то, что подпадает под определение "устранены" (большая часть из перечисленного, без сомнения, будет по достоинству оценена администраторами, а равно и пользователями, так что мы не предполагаем, что эти усовершенствования не ценны или не важны).

- ✓ Технологии управления **IntelliMirror.** IntelliMirror живет и здравствует в Windows 2003. IntelliMirror — это, собственно, не продукт, а скорее термин, используемый для обозначения общей выгоды, которую можно получить от использования в комплексе некоторых ключевых возможностей Windows 2000 или Windows 2003. Применение IntelliMirror становится возможным посредством использования активного каталога (Active Directory), набора политик групп (Group Policy), профайлов мобильных пользователей (Roaming Profiles) и служб удаленной инсталляции (Remote Installation Services — RIS).

  IntelliMirror устанавливает механизм регистрации обновлений для любой подходящей клиентской машины (которая может работать под управлением Windows 2003/2000/XP) и сохранения этих обновлений на сетевом сервере. Эта технология не только позволяет перестроить или восстановить конфигурацию исходной настольной системы, но также предоставляет пользователям возможность переходить с одной настольной системы на другую и при этом захватить с собой свои приложения, данные, предпочтения и установки настольной системы. Поскольку это уменьшает потребность в воссоздании сложных конфигураций и настроек, IntelliMirror должна в значительной мере снижать стоимость владения при сопровождении сложных современных систем.

- ✓ Поддержка широкого и **разнообразного** набора средств **управления.** Windows 2003 включает усовершенствованный и расширенный набор встроенных средств удаленного управления для сетей, настольных систем, серверов и других важнейших сетевых компонентов. Windows 2003 также работает с управляющими агентами и ПО от других поставщиков, таких как Tivoli Systems, Hewlett-Packard, NetQ, и с собственным сервером управления системами (Systems Management Server — SMS). Поскольку система Windows 2003 работает с ПО других поставщиков, стоимость сопровождения сложных современных систем должна значительно снизиться. Кроме того, многие новые средства администрирования, запускаемые из командной строки, можно использовать для создания мощных сценариев, которые автоматизируют выполнение многих задач.

- ✓ Легкость в освоении и использовании. За счет того, что Windows 2003 во многом напоминает гибрид Windows 2000 и Windows XP, Microsoft надеется сократить кривую обучения для тех, кто работал с предыдущими версиями Windows. Больше того, Windows 2003 включает многочисленные мастер-программы (wizards) и другие средства автоматизации, которые запоминают наиболее часто используемые поля (такие как имя пользователя и пароль) и могут предоставить их по запросу, когда входной контекст указывает на то, что подобные данные могут оказаться полезными. Настольные системы, работающие под управлением Windows 2003, также довольно дружественны, они отображают пункты меню Start, исходя из стереотипов использования; их легко реконфигурировать и настроить. За счет сокращения кривой обучения и повышения уровня практичности общие затраты на владение должны снизиться на уровне пользователя, где они обычно самые высокие.

- ✓ Удаленные **вычисления** для повышения продуктивности. Благодаря включению технологии терминального сервера, а также Web-ориентированных средств удаленного управления и администрирования, которые могут работать на любой настольной машине с подходящим установленным на ней Web-броузером, системы Windows 2003 стали более легкими в установке, конфигурировании и управлении в сравнении с более ранними версиями Windows. Это должно способствовать снижению стоимости владения для сетей; в особенности для тех сетей, в которых компетентность персонала на локальном уровне (скажем, в филиалах фирмы) может быть низкой или вовсе отсутствовать, но в которых можно применить "глобальные знания" сетевых администраторов и специалистов в удаленном режиме, чтобы справиться с ситуациями и разрешить проблемы, выходящие за пределы возможностей работников филиалов.
- ✓ Доступность и доступ в рамках всей сети. Сочетание Active Directory с его глобально доступными возможностями просмотра сетевых ресурсов, обращения к элементам управления доступом, службам безопасности и администрирования и Web-ориентированных возможностей средств конфигурирования и управления Windows 2003 облегчают администраторам установку и сопровождение сетей Windows 2003. Кроме того, конечным пользователям легче осуществлять навигацию по этим сетям и использовать их. За счет уменьшения затрат, связанных с подготовкой администраторов и конечных пользователей сети, Windows 2003 обещает значительное снижение стоимости владения, а также стоимости оборудования и ПО, обеспечивающих работу сети.

Существуют и другие возможности Windows 2003, которые помогают управлять TCO, помимо тех, которые мы перечислили выше. Учитывая проблемы пользователей, источником которых были более ранние реализации системы, и работая над тем, чтобы облегчить установку, настройку конфигурации и повседневную работу с Windows 2003, Microsoft создала пакет, преимущества которого действительно впечатляют. Хотя подобные преимущества иногда кажутся слишком малозаметными, они вполне реальны, когда речь идет о том, чтобы облегчить и упростить работу с сетью конечных пользователей и системных администраторов.

Более высокое быстродействие и надежность

Определение *более высокое быстродействие и надежность* охватывает множество возможностей Windows 2003, которые вносят вклад в увеличение производительности, доступности и надежности системы. Среди множества других позиций, относящихся к этой категории, наиболее заслуживают упоминания следующие.

- ✓ Возросший уровень системных ***проверок.*** Компания Microsoft провела больше собственных испытаний на большем количестве конфигураций аппаратного обеспечения для Windows 2003, чем для любой из предыдущих версий. Она также выпустила намного больше бета-версий (в том числе несколько для крупномасштабных производственных сетевых сред), чтобы воспользоваться преимуществами полученной от пользователей информации на этапе подготовки окончательной версии системы.
- ✓ Более жесткое управление памятью. Администратор виртуальной памяти (Virtual Memory Manager — VMM) системы Windows 2003 отличается большей надежностью по сравнению с более ранними версиями и обрабатывает недопустимые ссылки на память из приложений, системных компонентов и драйверов устройств лучше, чем. когда-либо прежде. Windows 2003 также включает механизм подписи для драйверов устройств, так что администраторы могут настроить конфигурацию системы таким образом, что она будет допускать работу только тех драйверов устройств, которые обладают действительной цифровой подписью.

- ✓ **Уменьшение количества необходимых перезагрузок и более быстрый перезапуск.** Windows 2003 требует перезагрузки только после выполнения около семи задач по конфигурированию системы; Windows NT должна перезагружаться после выполнения любой из свыше чем сорока задач по конфигурированию системы. Снижение требований к дампу памяти, опции запуска в безопасном режиме, более быстрая утилита проверки диска CHKDSK и средства автоматического восстановления системы также значительно облегчают перезапуск (или перекомпоновку) систем Windows 2003.

Полное использование преимуществ Active Directory

В рамках гибридных доменов, включающих серверы Windows 2003 и Windows NT, Active Directory может эмулировать доменную модель Windows NT с целью поддержки резервных контроллеров доменов (backup domain controller — BDC), ориентированных на Windows NT. Не забывайте о том, что Windows 2000 Server также обладает способностью эмулировать работу PDC для Windows NT. Active Directory также может поддерживать устаревшее сетевое клиентское ПО Windows, ориентированное на NetBIOS, и модели аутентификации в стиле давно ушедших времен сетевой ОС LAN Manager.

Использование этих возможностей в гибридных сетях означает, что вы можете в полной мере использовать собственные средства безопасности Windows 2003 на базе систем Kerberos или пользовательских сертификатов шифрования данных. Использование этих средств также означает отказ от доступа к полной структуре, которую может поддерживать лес из деревьев Active Directory, со стороны старых клиентов. (Леса, деревья, домены, узлы и производственные подразделения рассматриваются в главе 11.)

После того как все серверы сети будут переведены с Windows NT на Windows 2003 и Windows 2000. а все клиенты после обновления станут поддерживать Active Directory, возможности сервера Windows Server 2003 можно использовать значительно более полно. Функции административного управления можно определить для отдельных машин, групп машин, отдельных доменов или нескольких доменов. (В Windows NT администрирование доменов осуществляется скорее по принципу "все или ничего".)

Фактически в сети, которая является чисто сетью Windows 2003, приложения, способные работать с Active Directory, могут использовать каталог данных для поиска сетевых ресурсов (таких как файлы и принтеры), не требуя при этом никаких указаний от пользователя. Лучше всего то, что ресурсы на уровне домена, машины или на уровне отдельного ресурса могут контролироваться с помошью намного более мощных многоуровневых средств защиты. Помимо этого, системы Windows 2003 могут обеспечить более строгую аутентификацию, способную гарантировать, что идентификатор пользователя, используемый для запроса ресурсов, соответствует истинной личности того, кто запрашивает данный ресурс,

Большие сетевые возможности

Windows 2003 обеспечивает более совершенный сетевой доступ и надежность многими способами. Windows 2003 поддерживает использование нескольких сетевых адаптеров, при этом один или несколько адаптеров функционируют *в качестве горячего резерва* (*hot-standby capacity*). Это значит, что отказ основного интерфейса приводит к мгновенному переключению на вторичный интерфейс, что помогает обеспечить непрерывную доступность важных сетевых ресурсов в случае отказа адаптера или среды передачи данных. Windows 2003 также использует модель драйверов, общую для систем Windows 2000/XP/98, что тотчас делает доступными для использования в рамках Windows 2003 многочисленные высокоскоростные сетевые технологии и устройства. Подобный подход также служит для системных администраторов гарантией того, что драйверы для последних, более быстрых, новейших сетевых технологий будут готовы к использованию с Windows 2003 сразу после их выпуска.

Системы Windows 2003 также поддерживают сетевые технологии областей памяти с высокой пропускной способностью, такие как устройства Fiber Channel. Эти технологии позволяют обнаружить данные в любом месте сети и обеспечить постоянную готовность к вызову любого сервера либо для использования этих данных, либо для их поставки с целью удовлетворения клиентского запроса на обслуживание.

Сервер Windows Server 2003 также отличается усовершенствованными средствами удаленного доступа, улучшенной реализацией трансляции сетевых адресов (network address translation — NAT) и более совершенной терминальной службой (Terminal Services).

Усовершенствованный доступ к сети и Internet

Windows Server 2003 включает самый последний выпуск сервера Internet Information Server (IIS) версии 6.0. Это ПО пользуется преимуществами улучшенной производительности и надежности систем Windows 2003, чтобы обеспечить больший период работоспособности Web-служб. Помимо этого, улучшенная поддержка для технологии ASP (Active Server Pages — активные серверные страницы) облегчает Windows 2003 поддержку мощных Web-ориентированных приложений. Сервер *US* 6.0 отличается многими усовершенствованиями, включая более совершенную аутентификацию, управление ASP, элементы управления CGI (Common Gateway Interface — общий шлюзовой интерфейс), отказоустойчивость, возможности администрирования с использованием командной строки, управление ресурсами, безопасность и выравнивание нагрузки.

Системы Windows 2003 также содержат усовершенствованный набор прикладных служб, включая интерфейсы, которые уже поддерживают развитые серверные функции, такие как кластеризация, выравнивание нагрузки и обработка транзакций. Другими словами, системы Windows 2003 как никогда раньше облегчают создание мощных, надежных приложений, которые совместно используют данные и программы в рамках всей сети. Фактически все прикладные службы Windows 2003 готовы к использованию технологий Internet; это означает, что вы можете развернуть их с равным успехом внутри ЛС, интрасети (intranet) и экстрасети (extranet) либо в Internet.

Глава 9

Приготовиться, настроиться, пошла установка Windows 2003!

В этой главе...

- Обновление или установка с нуля
- Определим вычислительные возможности
- Пошаговая установка Windows Server 2003
- Установка Windows Server 2003 поверх другой ОС
- Установка Windows Server 2003 по сети
- Удаленная установка Windows Server 2003
- Использование утилит установки Windows Server 2003
- Устранение неразберихи
- Автоматизация установки

Установить Windows Server 2003 сравнительно легко, однако с начала установки до момента входа в систему это может отнять больше часа. Вы можете, однако, уменьшить многие задержки, если заранее все спланируете. Мы надеемся, что, следуя советам, приведенным в этой главе, вы избежите многих распространенных проблем установки, большинство из которых связано с отсутствием подходящего оборудования. Мы также предусмотрели раздел, посвященный поиску неполадок, чтобы обойти любые препятствия, которые встретятся на вашем пути.

Обновление или установка с нуля

Устанавливаете ли вы Windows Server 2003 с нуля или поверх существующей системы, планирование обеспечит вам беспрепятственную установку.

Обновление (upgrade), как ясно из самого термина, означает, что вы располагаете операционной системой, установленной на вашем компьютере, и желаете установить Windows Server 2003 *поверх* существующей операционной системы, сохранив при этом столько системных настроек, сколько возможно. Windows 2003 поддерживает обновление Windows NT со служебным пакетом SP5 или выше и обновление Windows 2000.

Обратите внимание, что также существуют способы обновления бета-версии Windows 2003. Если вы выбрали вариант установки Windows Server 2003 за счет обновления бета-версии этой ОС, мы настоятельно рекомендуем начать эту процедуру с создания резервных копий всех данных на каждой машине, которую вы планируете обновить. (Вопросов резервного копирования мы коснемся в главе 17.) Хотя вы можете перейти на Windows 2003 без потери существующих данных, аппаратное и программное обеспечение иногда ведут себя по-своему и могут спутать вам все карты. Чуточку предусмотрительности — и вы будете избавлены от реальных проблем!

Установка (installation) означает, что вы добавляете Windows 2003 на компьютер, на котором может присутствовать или отсутствовать другая операционная система. Для систем, на которых операционные системы существуют, вы можете выбрать вариант замены существующей ОС или создание системы с альтернативной загрузкой ОС. Система с альтернативной загрузкой ОС представляет собой компьютер, обладающий двумя или более операционными системами. При запуске у вас есть возможность выбрать, какая именно ОС будет загружаться. В некоторых конфигурациях с альтернативной загрузкой ОС данные одной ОС недоступны для другой (например, разделы NTFS ОС Windows Server 2003 недоступны из ОС Windows 95 или Windows 98).

Если вы устанавливаете Windows Server 2003 впервые, вам требуется принять некоторые решения, касающиеся конфигурации сервера, прежде чем вы приступите к установке ПО. Существуют три основных способа установки Windows Server 2003.

- ✓ **С компакт-диска.** Этот тип установки требует наличия компьютера с установленным на нем локальным дисководом для компакт-дисков. Установка с компакт-диска не требует сетевого адаптера, но если вы планируете подключить систему к сети, лучше, если во время установки адаптер будет на своем месте. В данной главе мы остановимся на этом типе установки.
- ✓ **По сети.** Этот тип установки требует сетевого доступа и чтобы файлы компакт-диска были доступны на сети. Доступ к сети можно получить либо посредством существующей ОС, либо с помощью загрузочной дискеты.
- ✓ **Автоматическая.** Этот тип установки требует внесения информации по установке в файл данных, который вы можете затем объединить с файлом сценария для выполнения.

Запуск программы установки Windows Server 2003 можно осуществить несколькими способами.

- ✓ **Установка с загрузочного компакт-диска.** Если ваш компьютер позволяет осуществлять загрузку с устройства для чтения компакт-дисков, вы можете загрузить программу установки Windows 2003 с компакт-диска.
- ✓ **Установка с загрузочной дискеты.** Если в вашем распоряжении нет загрузочного дисковода компакт-дисков, вы можете осуществить загрузку с дискеты. Однако средство создания установочной дискеты больше не включается в состав компакт-диска; вам следует загрузить его из раздела Windows 2003 Web-узла Microsoft. Чтобы отыскать средство создания установочной дискеты, укажите Web-броузеру адрес `www.microsoft.com/windowsserver2003/`, а затем выполните поиск по ключевым словам *setup disks*.
- ✓ **Установка с компакт-диска при наличии другой ОС.** Если существующая ОС на вашем компьютере предоставляет вам доступ к устройству чтения компакт-дисков, вы можете установить Windows 2003 без загрузочной дискеты. (Более подробно этот способ описан ниже, в разделе, посвященном пошаговой установке Windows 2003.)
- ✓ **Установка по сети.** Вы можете воспользоваться этим способом, если файлы установки Windows 2003 доступны на другом компьютере в сети. Файлы могут размещаться на разделяемом дисководе компакт-дисков, либо копия содержимого дистрибутивного компакт-диска может помещаться на сетевом диске. Подробности этой процедуры описаны ниже, в разделе, посвященном сетевой установке.

- ✓ **Удаленная установка.** Microsoft предлагает процедуру удаленной установки ОС под названием RIS (Remote Installation Service — служба удаленной установки), которая позволяет сетевому администратору "продвинуть" установку Windows 2003 в сеть. *(Продвижение установки* означает, что администратор может развернуть Windows 2003 в сети, не посещая каждого клиента для запуска процедуры установки.)

Подготовка к битве

Прежде чем приступить к установке, необходимо кое-чем запастись. Мы предлагаем следующий перечень подобных вещей, чтобы помочь вам собрать информацию и подобрать оборудование, необходимое для установки. Программа Setup Windows 2003 не требует наличия всех элементов, которые мы привели в следующем разделе, но когда мы выполняем установку, то предпочитаем иметь все под рукой.

Руководства

Ниже приведен список книг, которые вам желательно было бы иметь под рукой (это, конечно, наиболее важные книги).

- ✓ **Руководства по Windows 2003,** В некоторых случаях руководства по Windows 2003 входят в комплект поставки в отпечатанном виде; в других случаях они доступны только в электронной форме на дистрибутивном компакт-диске или интерактивно на Web-узле компании Microsoft по адресу:
  `www.microsoft.com/windowsserver2003/.`
- ✓ **Руководства по оборудованию компьютера.** Это руководства по базовой машине и дополнительным компонентам или периферийным устройствам, на которых вы планируете установить Windows 2003. В особенности желательно иметь руководства для ваших сетевых и видеоплат.
- ✓ **Руководство по модему (необязательно).** Это руководство понадобится, только если вы планируете установить на сервере один или несколько модемов.

Программное обеспечение

Если вы не желаете внезапно обнаружить, что у вас чего-то недостает, позаботьтесь о том, чтобы иметь следующее ПО.

- ✓ **Компакт-диск Windows Server 2003.** Это CD-ROM, который поставляется с сервером Windows Server 2003. Вам также необходим код компакт-диска (или код продукта), который обычно наносится на этикетку, приклеиваемую к футляру компакт-диска.
- ✓ **Компакт-диск со служебными пакетами Windows Server 2003 или соответствующие загруженные файлы.** Не следует ожидать выхода служебного пакета (иногда называемого также пакетом обновления) для Windows 2003 по меньшей мере в течение трех месяцев после ее официального выпуска. До тех пор вы можете пропустить раздел "Служебные пакеты Windows 2003", приведенный ниже.
- ✓ **Драйвер сетевого адаптера.** Программа Setup Windows 2003 должна обнаружить адаптер на сервере, но на всякий случай держите под рукой дискету с необходимыми драйверами.
- ✓ **Драйверы SCSI-интерфейса.** Программа Setup Windows 2003 должна распознать все SCSI-устройства, если они приведены в списке HCL (Hardware Compatibility List — перечень совместимого оборудования) на Web-узле (`www.microsoft.com/hwdq/hcl/`). И вновь держите под рукой дискету с драйверами.

Оборудование

Естественно, установка Windows Server 2003 также требует некоторого аппаратного обеспечения, перечисленного ниже.

- ✓ **Компьютер.** Убедитесь в том, что ваш компьютер соответствует перечню HCL. Помните, что вам необходим как минимум процессор с частотой 133 МГц, но мы думаем, вас вряд ли удовлетворит что-то медленнее, чем 550 МГц. Вам также необходима мышь, подключенная к компьютеру, — она просто облегчает жизнь!
- ✓ **Оперативная память.** Чем больший объем ОП вы можете себе позволить, тем лучше. Минимум, который вам необходим, — 128 Мбайт, однако вы достигнете лучших результатов, имея в своем распоряжении 256 или 512 Мбайт.
- ✓ Дисковод **компакт-дисков.** Если вы устанавливаете Windows Server 2003 с компакт-диска, вам необходимо устройство чтения компакт-дисков. В более поздних моделях компьютеров это устройство входит в последовательность устройств, с которых может осуществляться загрузка компьютера. Это дает вам возможность установить Windows 2003 с компакт-диска.
- ✓ **Жесткий диск.** На вашем жестком диске должно быть по меньшей мере 1,5 Гбайт свободного пространства, однако, мы полагаем, вам не стоит даже начинать процедуру, имея меньше 4 Гбайт.
- ✓ **Модем.** Если сервер подключается к Internet или обеспечивает доступ к удаленным пользователям, одним из способов обеспечить такое подключение является модем (внутренний либо внешний). Мы отдаем преимущество модемам со скоростью не меньше 56 Кбит/с.
- ✓ **Видеооборудование.** Вам требуются адаптер VGA или адаптер с более высоким разрешением и монитор. Мы рекомендуем видеоадаптер SVGA.
- ✓ **Кабели.** В зависимости от устанавливаемых компонентов вам могут потребоваться кабели для модема, телефонные кабели, шнуры питания, кабели для монитора и др.

Информация

Во время установки вам придется неоднократно выбирать одну из нескольких альтернатив. Ваш выбор будет более обоснованным, если прежде, чем вы начнете установку, вы будете представлять себе, как отвечать на вопросы о выборе того или иного варианта. Рассмотрим пункты следующего списка.

- ✓ **Файлы SERVER1.TXT — SERVER4.TXT.** В подкаталоге `\docs` инсталляционного компакт-диска Windows Server 2003 содержится несколько файлов, включающих самую свежую информацию и подробности, касающиеся установки, которые были собраны слишком поздно, чтобы поместить их в печатный вариант руководств. Исследуйте их на предмет полезной информации.
- ✓ NTFS (New Technology File System — файловая система новой технологии) — родная файловая система Windows 2003, которая значительно более надежна, чем файловая система FAT (File Allocation Table — таблица размещения файлов). Если вам не требуется обратная совместимость со старыми ОС Microsoft на одной и той же машине с конфигурацией с альтернативной загрузкой, нет никакой необходимости использовать файловую систему FAT.

- ✓ **Лицензирование.** Вам необходимо знать, каким образом были приобретены Windows Server 2003 и клиентские лицензии, поскольку программа Setup Windows 2003 запрашивает вас, желаете ли вы использовать лицензирование в расчете на сервер (per-server) или в расчете на рабочее место (per-seat).
- ✓ **Имя компьютера.** Каждый компьютер нуждается в уникальном имени, которое вы можете легко распознать в сети.
- ✓ **Имя рабочей группы/домена.** Если ваш сервер — первый контроллер домена, устанавливаемый в сети, вы должны создать имя домена. Если ваш компьютер входит в текущий домен, в котором контроллер домена уже существует, более рационально подключить этот компьютер к сети с доступом к этому домену. Если вы устанавливаете Windows 2003 в рамках рабочей группы, вам необходимо имя рабочей группы. Помните, что для этого установочного параметра действует правило "либо–либо", но вы всегда можете передумать позже.
- ✓ **Протоколы.** Информация, касающаяся протоколов, прежде всего определяет, какие протоколы использует (или будет использовать) компьютер в процессе сетевого взаимодействия. Если вы планируете использовать протокол TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Internet), за подробностями обратитесь к главе 14. Определитесь, будете ли вы настраивать конфигурацию протокола TCP/IP вручную или автоматически посредством DHCP-сервера (Dynamic Host Configuration Protocol — протокол динамической конфигурации узлов). Если этот сервер подключается к Internet, убедитесь в том, что ваш IP-адрес верно установлен.
- ✓ **Возможности удаленного соединения.** Определите, подключается ли (или будет подключаться) ваш сервер к Internet, или он будет выполнять роль Web-сервера. В последнем случае вы можете установить IIS-сервер, чтобы обеспечить возможности сетевого взаимодействия через Web-службы и RAS-службы (Remote Access Service — сервис удаленного доступа). RAS-службы также дают возможность вашим пользователям и клиентам подключаться к сети по коммутируем каналам. Вы всегда можете также установить Web- и RAS-службы позднее. В любом случае вам необходимо работающее Internet-соединение.
- ✓ **Роли сервера.** Правила игры меняются в зависимости от того, какие роли может играть сервер в процессе поддержки домена. Функции вашего сервера могут оказывать влияние на установку Windows Server 2003, однако теперь это не жизненно важное решение, поскольку конфигурация сервера не настраивается до тех пор, пока не будет завершена начальная установка. Более подробно об этом можно прочитать в главах 11 и 12.

Мощь вашего сервера

Прежде чем устанавливать Windows Server 2003 (независимо от того, выполняете ли вы обновление или установку с нуля), вам необходимо ознакомиться с минимальными требованиями Microsoft к аппаратному обеспечению. Если ваш сервер не удовлетворяет этим требованиям по самому минимуму, ваша установка может прерваться посередине и оставить вас в совершенном расстройстве.

Компания Microsoft в своих минимальных требованиях чересчур снисходительна, поэтому мы предоставляем в ваше распоряжение более реалистичные цифры, чтобы удовлетворить реальные потребности. Если вы будете следовать рекомендациям Microsoft, все может закончиться тем, что сервер будет неработоспособным. В табл. 9.1 приведены цифры Microsoft в сравнении с нашими реальными цифрами.

Таблица 9.1. Минимальные требования: от **Microsoft** и от **"чайников"**

Элемент	Требования Microsoft	Реальные требования
Процессор	133 МГц	550 Мгц и выше
Оперативная память	128 Мбайт	256 Мбайт и выше
Монитор	VGA	SVGA и выше
Сетевой адаптер	Отсутствуют*	Один (по меньшей мере 32-разрядный)
Компакт-диск	Отсутствуют	Накопитель CD-ROM (12х или выше) или DVD
Жесткий диск	Свыше 1,5 Гбайт	4 Гбайт и выше
Флоппи-диск	3,5 дюйма	3,5 дюйма (HD — высокоплотный)

**Сетевой адаптер требуется для прямого сетевого доступа. Если адаптер* отсутствует во время установки, вы можете установить его позднее.

Вы можете придерживаться минимальных требованиями от Microsoft, но это закончится тем, что многие функции вашего сервера станут ужасно медленными и неподатливыми. Например, хотя Windows Server 2003 поддерживает мониторы с низким разрешением, вы должны использовать монитор с высоким разрешением (SVGA или выше) из-за наличия у Windows 2003 развитого GUI-интерфейса (Graphical User Interface — графический интерфейс пользователя). Во многих случаях чем больше дискового пространства, оперативной памяти, мощности процессора и т.д., тем лучше. Приобретайте столько, сколько выдержит ваш бюджет, чтобы вам не пришлось слишком быстро обновлять оборудование сервера.

Посетите Web-узел Microsoft, в частности страницы, посвященные Windows Server 2003 (`www.microsoft.com/windowsserver2003/`). Здесь вы найдете документы и FAQ-файл, содержащие ответы на распространенные вопросы по многим темам, таким как лицензирование, минимальные требования и обновления. Если вам этих ответов будет недостаточно, откройте первую страницу FAQ-узла Microsoft (`www.ntfaq.com`), на которой содержится информация по системам Windows 2003.

Windows 2003: это изобилие утилит

Ни одна отдельно взятая ОС не выполняет всех требований пользователей. Программисты и другие знатоки вычислительной техники обычно разрабатывают небольшие сценарии или программы для выполнения функций, которые не включает базовая ОС. Утилиты Windows 2003 наличествуют в большом количестве из-за их популярности. Вы можете найти многие из этих утилит, в особенности средства инсталляции, в Internet на популярных Web-узлах, посвященных Windows 2003 и Windows NT, таких как `http://windowsnt.about.com` и `www.bhs.com`.

В некоторых случаях одно и то же средство, которое используется в Windows 9x/NT/2000, будет работать и с Windows Server 2003. Однако это не всегда справедливо. Прежде чем использовать приложение в ситуациях, где возможна потеря данных, следует проверить, как оно работает с Windows 2003.

Компания Microsoft поставляет набор инструментальных средств Windows Server 2003 Resource Kit, который вы можете приобрести по Internet или в книжном магазине. Пакет включает утилиты для установки, управления файлами, устранения неполадок и планирования.

Еще один важный момент, который следует проконтролировать, — это принадлежность вашего сервера списку HCL от Microsoft. Испытательная лаборатория Microsoft тратит немало времен, испытывая продукты на совместимость с Windows 2003. Получение сертификата лаборатории Microsoft означает, что организация может поместить логотип Microsoft на своих продуктах. Microsoft включает списки сертифицированных продуктов в перечень HCL.

Выбор в качестве сетевого сервера одного из серверов, перечисленных в списке HCL, помогает гарантировать наиболее беспрепятственную установку, поскольку вы знаете, что компания Microsoft уже испытала и сертифицировала этот продукт. Сертификация продуктов для включения в список HCL — постоянная задача Microsoft, и компания поддерживает и обновляет список HCL для всех версий своих существующих ОС на Web-узле www.microsoft.com/hwdq/hcl/.

Если вы не уверены в совместимости системы в целом или определенного компонента, вы можете либо поискать ее в списке HCL, либо воспользоваться автоматической системой проверки совместимости прямо на компакт-диске. Вставьте компакт-диск в дисковод системы с существующей ОС Windows (если экран приглашения не появится автоматически, запустите из корневого каталога компакт-диска программу sturtup.exe). Выберите опцию Check System Compatibility (Проверить совместимость системы), а затем опцию Check My System Automatically (Проверить систему автоматически). После этого загрузится мастер-программа проверки, которая сделает запрос о необходимости загрузки файлов обновления- Если у вас есть доступ к Internet, это средство может само обновиться с использованием более поздней и наиболее значительной версии списка HCL прежде, чем приступить к обследованию вашей системы. При обнаружении некоторых проблем или несовместимости программа выведет на экран список проблем.

Шаг за шагом: установка Windows 2003

В этом разделе мы рассмотрим всю процедуру установки Windows Server 2003 — экран за экраном. К сожалению, мы не можем представить экраны для всех возможных типов установки, так что в этом разделе мы приведем инструкции по одному типу инсталляции: с загрузочного компакт-диска.

Подготовка сервера

Первая главная задача по загрузке ПО в систему — подготовить сервер к процессу установки. Вообще, эти вопросы вы должны решить до того, как приступите к установке Windows Server 2003.

1. **Убедитесь в том, что все оборудование соответствует перечню HCL.**

   Хотя возможна установка Windows 2003 на систему, некоторые компоненты которой отсутствуют в перечне HCL, это не всегда легко сделать. Короче говоря, если оборудование не соответствует списку HCL, вам нежелательно держать его в вашей системе.

2. **Установите на сервер сетевой адаптер.**

   К счастью, Windows 2003 поддерживает технологию Plug-and-Play, так что большинство плат можно сменить на лету, — если только ваша плата не настолько устарела, что по-прежнему использует двухрядные переключатели или перемычки (dual in-line package — DIP).

3. **Если вы желаете подключить сервер к внешним источникам, таким как Internet, установите внутренний модем.**

Пошаговая установка Windows 2003

Приведенные ниже шаги детально описывают процесс установки Windows 2003 с загрузочного компакт-диска. На протяжении всего процесса установки мы принимаем опции, используемые по умолчанию. Итак, приготовьтесь.

Ваша система должна быть сконфигурирована таким образом, чтобы ее загрузка осуществлялась с компакт-диска. Это достигается за счет внесения изменений в CMOS-память. Чтобы узнать, как вводить, редактировать и сохранять параметры CMOS, обратитесь к документации производителя материнской платы вашего компьютера.

1. **Вставьте компакт-диск Windows Server 2003 в устройство чтения компакт-дисков и загрузите компьютер. Если вам предлагают нажать клавишу для загрузки с компакт-диска, сделайте это.**

   Появится серый экран GUI, на котором отображается список пяти основных процессов установки Collection information (Сбор информации), Dynamic Update (Динамическое обновление), Preparing installation (Подготовка к установке), Installing Windows (Установка Windows) и Finalizing installation (Завершение установки). Кроме того, автоматически запускается программа Windows Setup Wizard (Мастер установки Windows).

2. **Выберите тип установки по умолчанию, который отображается в окне New Installation (Advanced) (Новая установка (*Дополнительно*)), а затем щелкните на кнопке Next** (Далее).

   Появится окно License Agreement (Лицензионное соглашение).

   Работая с GUI-мастером, будьте очень внимательны. Зачастую, после того как вы щелкнете на кнопке Next, чтобы продолжить процесс, у системы уходит несколько секунд (иногда до минуты) на смену отображения. Не пытайтесь щелкнуть на кнопке Next еще раз, даже если вы подозреваете, что случайно пропустили это действие. Если вы щелкнете на кнопке Next дважды, вы пропустите экран и кнопка Back (Назад) перестанет работать (в некоторых местах кнопка Back блокируется), Если вы подождете приблизительно пять минут и система не сменит отображение, попробуйте щелкнуть на кнопке Next еще раз.

3. **Прочтите лицензионное соглашение, щелкните на опции I Accept this Agreement (Я принимаю это соглашение), а затем щелкните на кнопке Next**

   Появится экран Your Product Key (Код продукта).

4. **Введите 25-символьный код продукта, а затем щелкните на кнопке Next.**

   Появится окно Setup Options (Параметры установки), в котором вы можете выбрать варианты установки и доступности, а также установить язык и страну.

   Код продукта обычно находится на этикетке, приклеенной к футляру компакт-диска.

5. **Для копирования и установки файлов воспользуйтесь опциями, заданными по умолчанию. Если вам требуются специальные возможности, обеспечивающие доступность во время установки, такие как Magnifier (Увеличение) или Narrator (Диктор), щелкните на кнопке Accessibility Options (Специальные возможности) и выберите подходящий параметр. Если принимаемые по умолчанию региональные и языковые установки вам не подходят, выберите новый вариант из выпадающего списка. Для продолжения щелкните на кнопке Next**

Появится экран Get Updated Setup Files (Получить обновленные файлы установки).

6. **Если вы имеете доступ к Internet, щелкните на опции Yes, Download the Updated Setup Files (Да, загрузить обновленные файлы установки), а затем щелкните на кнопке Next. Если у вас нет доступа к Internet, щелкните на опции No, Skip this Step and Continue Installing Windows (Нет, пропустить этот шаг и продолжить установку Windows), затем щелкните на кнопке Next.**

   Если вы выберете опцию Yes (Да), утилита Dynamic Update (Динамическое обновление) загрузит обновленные файлы инсталляции.

   Программа установки скопирует инсталляционные файлы и перезапустит компьютер в текстовом режиме. В конце концов, процедура установки Windows Server 2003 выведет следующее приглашение.

```
Welcome to "Setup
This portion of the setup program prepares Microsoft ®
      . Windows ,2003 ™ to run on your computer.
*To set up Windows now, press ENTER.
*To Repair a Windows installation using Recovery Console, •
 press R.
*To quit Setup without installing Windows, Press F3.
.(Добро •пожаловать.в программу установки.
 Этот фрагмент программы установки подготавливает
 Microsoft ® Windows 2003 ™ для работы на вашем компьютере.
*Чтобы начать установку, нажмите клавишу <Enter>.
*Чтобы возвратиться к установке Windows, используя кон- -
 соль восстановления, нажмите клавишу <R>.'
*Чтобы выйти из программы установки без инсталляции
 Windows, нажмите клавишу <F3>.)
```

7. **Нажмите клавишу <Enter>.**

   Программа установки предложит вам выбрать диск и раздел, в который будет инсталлироваться Windows Server 2003.

8. **Для выбора раздела жесткого диска воспользуитесь клавишами со стрелками, а затем выполните следующие действия.**

   - Если вы намерены использовать все свободное место на диске для загрузочного раздела Windows, нажмите клавишу <Enter> после выбора расположения раздела.
   - Если вы намерены использовать только часть свободного места на диске для загрузочного раздела Windows, нажмите клавишу <C>. После этого вам будет предложено ввести в приглашение для ввода размер создаваемого раздела. Введите значение в пределах от единицы до максимальной величины раздела, доступного на диске, а затем нажмите клавишу <Enter>. Вновь созданный раздел появится в списке дисков и разделов как новый ("New (Unformatted)"). Выберите этот новый раздел и нажмите клавишу <Enter>.
   - Если вам необходимо удалить существующий раздел, выберите его, а затем нажмите клавишу <D>. Вам будет предложено подтвердить намерение об удалении раздела. Нажмите клавишу <L>, и раздел будет удален.

Обычно вы намерены выбрать первый диск системы и первый свободный раздел для загрузочного диска Windows. Также вы должны создать раздел размером не меньше 1,5 Мбайт, где будет размещаться Windows 2003 (мы, однако, рекомендуем как минимум 4 Гбайт).

9. **Когда программа установки запросит вас о файловой системе, с использованием которой вы намерены отформатировать выбранный раздел, выберите NTFS, а затем нажмите клавишу <Enter>.**

   Программа установки тратит значительное время на форматирование диска, в особенности, если раздел большой. После завершения форматирования программа установки проверит ваши жесткие диски, создаст список файлов, а затем скопирует огромное количество файлов с компакт-диска во вновь отформатированный файл. Здесь время ожидания может растянуться надолго, поэтому смените моторное масло, приготовьте кофе или научитесь обметывать края при шитье,

10. **Когда вы увидите сообщение о том, что система будет перезагружена, нажмите клавишу <Enter> для немедленной перезагрузки или подождите 15 секунд, пока процесс установки не выполнит перезагрузку автоматически.**

    Убедитесь в том, что в устройстве для флоппи-дисков нет дискеты. Также не нажимайте клавишу для загрузки с компакт-диска. Если ваш компакт-диск загружается автоматически, а не требует нажатия клавиши для инициирования загрузки, вытащите компакт-диск перед перезагрузкой.

    После перезагрузки программа установки Windows 2003 вновь входит в режим использования GUI-интерфейса, просматривает диск в поисках устройств и устанавливает соответствующие драйверы.

11. **Если вы живете в США, после появления экрана Regional and Language Options (Языки и стандарты) подтвердите установки, используемые по умолчанию, и щелкните на кнопке Next. В противном случае внесите необходимые изменения с помощью кнопки Customize (Настройка) или Details (Подробности), а затем щелкните на кнопке Next.**

12. **Когда программа установки предложит ввести ваше имя и название вашей организации, введите необходимую информацию, а затем щелкните на кнопке Next.**

    Если вы используете сервер в личных целях, можете не вносить название организации.

13. **Когда программа установки попросит вас выбрать тип используемого лицензионного соглашения, щелкните на одной из опций: Per Server (На сервер), Per Device (На устройство) или Per User (На пользователя), а затем щелкните на кнопке Next.**

    Прежде чем вносить отметки в этот раздел, проверьте ваш заказ на покупку, чтобы выяснить, какую именно лицензию вы приобрели. Лицензии в расчете на устройство или на пользователя обычно используются для сетей предприятий, а лицензии в расчете на сервер — для небольших сетей. Вы можете сменить тип лицензирования в расчете на сервер на лицензирование в расчете на устройство или пользователя только один раз, поэтому, прежде чем продолжить, внимательно проанализируйте этот параметр установки.

Если вы не уверены, какую опцию выбрать, выберите Per Server. Убедитесь в том, что параметр Number of Concurrent Connections (Количество одновременных соединений) установлен правильно. По умолчанию его значение равно 5.

14. **Когда программа установки предложит вам ввести имя компьютера и пароль для административной учетной записи пользователя, введите их и щелкните на кнопке Next.**

Если ваша организация применяет соглашение об именовании, убедитесь в том, что выбранное вами имя компьютера удовлетворяет этим правилам.

Пароль административной учетной записи должен быть сложным и состоять не менее чем из шести символов, желательно в верхнем и нижнем регистре, и как минимум с одним цифровым или не алфавитно-цифровым символом. Да, именно таким и должен быть ваш пароль, если вы не хотите, чтобы его легко вычислили.

15. **Если программа установки запрашивает у вас информацию о наборе номера, введите корректную информацию по набору номера, а затем щелкните на кнопке Next.**

Программа установки запросит информацию о наборе номера. Если она обнаружит в вашем компьютере модем, в большинстве случаев вам необходимо предоставить только региональный код.

16. **Введите правильную дату, время и информацию о часовом поясе в соответствии с вашим местоположением и щелкните на кнопке Next**

Программа установки продолжит загружать драйверы для обнаруженных сетевых компонентов.

17. **Решите, желаете ли вы принять параметры по умолчанию или настроить параметры для вашей сети.**

Типичные параметры настраивают протокол TCP/IP на использование службы динамической конфигурации DHCP. Если ваша сеть предоставляет эту услугу и требуется применение этой системы, используйте параметры, принимаемые по умолчанию.

Если вам необходимо задать IP-адрес, маску подсети и используемый по умолчанию шлюз, выберите индивидуальные параметры.

18. **Если вы настраиваете параметры, выполните следующие действия.**

    а) **Выберите опцию** Custom Settings **(Индивидуальные параметры), а затем щелкните на кнопке** Next.

    Программа установки отобразит имя обнаруженного сетевого адаптера и перечень нескольких служб, устанавливаемых по умолчанию: Client for Microsoft Networks (Клиент для сетей Microsoft), Network Load Balancing (Выравнивание загрузки сети), File and Printer Sharing for Microsoft Networks (Служба доступа к файлам и принтерам сетей Microsoft) и Internet Protocol (TCP/IP) (Протокол Интернета).

    б) **Выберите элементы** Internet Protocol (TCP/IP) **(Протокол Интернета), а затем щелкните на кнопке** Properties (Свойства).

    Появится диалоговое окно Internet Protocol (TCP/IP) Properties.

    в) **Щелкните на опции Use** the Following IP Address **(Использовать следующий IP-адрес).**

г) **Введите IP-адрес, маску подсети и шлюз, используемый по умолчанию.**

д) **Щелкните на кнопке** OK.

19. **Если вы будете использовать установки, принятые по умолчанию, выполните следующее.**

    а) Выберите опцию Typical Settings (Типичная).

    б) Щелкните на кнопке Next.

    Программа установки предложит вам ввести имя рабочей группы или домена, в состав которой она будет входить.

20. **В ответ на вопрос** о **том,** будет **ли ваш компьютер частью домена, выполните одно из следующих действий.**

    - **Если система будет входить в рабочую группу, щелкните на опции No (Нет), введите имя рабочей группы (по умолчанию принимается имя WORKGROUP), а затем щелкните на** Next
    - **Если система будет входить в состав домена, щелкните на опции** Yes (Да), **введите имя и щелкните на** Next. **Введите учетную запись и пароль уровня администратора (по необходимости), затем щелкните на кнопке OK.**

    Программа установки скопирует и настроит конфигурацию компонентов системы, а затем подстроит меню Start (Пуск) и реестр. Пока это происходит, вы ждете. Продолжайте ждать, ждать и ждать. (Поскольку ничего другого вам не остается делать.)

    После того как программа установки завершит эту часть работы, вы увидите сообщение о том, что система будет перезагружена. Вы можете нажать клавишу <Enter>, чтобы система перезагрузилась немедленно, или подождать 15 секунд, пока процесс установки дойдет до автоматической перезагрузки. После перезагрузки появится раскрывающееся окно приветствия Welcome (Знакомство с Windows 2003).

21. **Для отображения диалогового окна Log On to Windows (Вход в Windows) нажмите комбинацию клавиш <Ctrl+Alt+Del>.**

22. **Введите пароль для учетной записи администратора, а затем для входа в систему щелкните на кнопке OK.**

Спустя несколько мгновений появится рабочий стол Windows Server 2003 — верный знак, что вы успешно установили Windows Server 2003! (Просто для того, чтобы поддержать вашу решимость, Windows Server 2003 автоматически запускает мастера настройки конфигурации сервера, подготавливая следующий пакет задач. Чтобы узнать больше об этой мастер-программе, обратитесь к главе 10.)

Если скопировать подкаталог i386 с компакт-диска вашей системы Windows Server 2003 на вновь установленный сервер, драйверы и другие ресурсы сразу станут доступны вам, так что позже вы сможете при желании добавить необходимые службы и ресурсы. Если вы не последуете этой рекомендации, то вам придется вставлять компакт-диск всякий раз, когда вам потребуется добавить ресурсы и службы к этой машине.

Установка поверх существующей ОС

Если на вашем компьютере уже установлена операционная система с доступом к компакт-диску, такая как DOS, Windows 3.*x*, Windows for Workgroups, Windows 9.*x*, Windows NT, Windows 2000 или Windows XP, вы можете запустить установку Windows Server 2003 из этой ОС. Это единственный способ установки с обновлением, т.е. модернизации ОС. Если вы запускаете установку с загрузочного компакт-диска, автоматически выполняется полная установка.

Хотя вы можете начать установку Windows Server 2003 из DOS, Windows *3.x,* Windows for Workgroups, Windows 9.*x*, вы не можете модернизировать их до уровня сервера Windows Server 2003. Независимо от существующей ОС для установки Windows Server 2003 вы должны удовлетворить минимальные требования к оборудованию, которые не достижимы в системах, работающих под управлением ОС Windows 9.*x* или более ранних версий.

Для установки с компакт-диска запустите одну из следующих команд с помощью приглашения для ввода командной строки или диалогового окна Run (Выполнить).

- ✓ Если вы пользуетесь 16-разрядной ОС наподобие DOS, Windows 3.*x* или Windows for Workgroups, вам необходимо использовать команду

  ```
  <буква для устройства CD-ROM>:\i386\winnt
  ```

- ✓ Если вы пользуетесь 32-разрядной ОС, такой как Windows *9.x,* Windows NT, Windows 2000 или Windows XP, и возможность автозапуска отключена, вам необходимо использовать команду

  ```
  <буква для устройства CD-ROM>:\i386\winnt32
  ```

Если вы попытаетесь запустить неверную программу установки, сервисная программа подскажет, что необходимо просто запустить другую программу.

Если автозапуск включен, вы увидите экран приветствия мастера установки Windows Server 2003 (Welcome to Windows Setup wizard).

После того как появится текстовый экран DOS, запрашивающий подтверждения расположения файлов дистрибуции, запуск программы установки вручную из DOS, Windows *3.x* или Windows for Workgroups требует от вас выполнить следующее.

1. **Убедитесь в том, что отображается верный путь к каталогу i386 на дистрибутивном компакт-диске, а затем нажмите клавишу <Enter>.**

   Программа установки скопирует файлы с компакт-диска на жесткий диск вашего компьютера.

2. **После того как программа установки проинформирует вас о том, что копирование всех файлов завершено, чтобы перезагрузиться и продолжить, нажмите клавишу <Enter>.**

Когда машина перезагрузится, программа установки продолжит работу с шага 8, описанного выше, в разделе "Установка Windows 2003: пошаговый разбор".

Если вы вставите компакт-диск с Windows Server 2003 в дисковод доя компакт-дисков на компьютере с установленной операционной системой с включенной опцией автозапуска (например, Windows NT), появится раскрывающееся окно с запросом о том, действительно ли вы желаете модифицировать систему до Windows 2003. Если вы щелкнете на кнопке Yes, вам не придется вручную искать и запускать программу WINNT или WINNT32.

Для запуска программы установки из Windows 9.x, Windows **NT,** Windows 2000 или Windows XP выполните следующие действия.

1. На экране Welcome to Windows Setup Wizard выберите опцию New Installation (Advanced) и щелкните на кнопке Next.
2. **Прочтите лицензионное соглашение. Выберите опцию I Accept This Agreement, а затем щелкните на кнопке Next.**
3. **Введите код продукта, а затем щелкните на кнопке Next.**

   Появится окно Setup Options (Параметры установки).
4. **Щелкните на кнопке Advanced Options (Дополнительные параметры).**
5. **Замените папку Installation Folder (Папка установки), если используемая по умолчанию не подходит.**
6. **Для установки Windows 2003 в раздел, отличный от того, где размещена текущая ОС (настоятельно рекомендуется), убедитесь в том, что во время установки выбрана опция I Want to Choose the Install Drive Letter and Partition (Выбрать раздел диска для установки).**
7. **Щелкните на кнопке OK.**
8. **Щелкните на кнопке Next**

   Программа установки скопирует файлы с компакт-диска на жесткий диск. Перед тем как автоматически перезагрузить компьютер, она дает 10-секундную задержку.

   После того как машина перезагрузится, программа установки продолжит работу с шага 8, описанного ранее, в разделе "Установка Windows 2003: пошаговый разбор".

Установка по сети

Установка Windows Server 2003 по сети во многом похожа на то, как выполняется установка с локального компакт-диска. Оба метода требуют доступа к файлам дистрибуции с компакт-диска, и вы должны вручную запустить средства установки WINNT и WINNT32.

Запуск программы установки из DOS, Windows 3.x или Windows for Workgroups вручную требует небольших изменений в процессе, описанном в предыдущем разделе. Однако применительно к этим ОС вам требуется отобразить букву локального диска на общий сетевой ресурс. (Эта отображаемая буква говорит программе установки, где находятся файлы дистрибуции.) Программа установки автоматически скопирует все файлы данных, которые ей необходимы перед перезагрузкой компьютера.

Запуск вручную программы установки из Windows 9.x, Windows **NT,** Windows 2000 или Windows XP по сети требует дополнительного независимого переключателя. Убедитесь в том, что в диалоговом окне Advanced Options (которое появляется после щелчка на кнопке Advanced Options экрана Setup Options в процессе установки) выбрана опция Copy all Installation Files from Setup CD (Копировать все файлы с CD-ROM на жесткий диск).

Удаленная установка

Компания Microsoft разработала новый процесс инсталляции, называемый службой удаленной установки (Remote Installation Service — RIS). Эта служба позволяет сетевому администратору распространить установку Windows 2003 по сетевой системе. Хотя этот процесс, в общем, упрощает множественные установки, это — непростое дело. Он требует установки

и настройки конфигурации нескольких ключевых служб, помимо службы RIS, а именно: службы имен доменов (Domain Name Service — DNS), DHCP и Active Directory.

Клиенты, которые желают, чтобы установка Windows Server 2003 "дошла" до них по сети, должны обладать адаптером, совместимым со "предзагрузочной" средой расширения (Preboot Extension Environment — PXE), или загружаться с помощью специального сетевого клиентского загрузочного диска.

Если вы желаете детально изучить процедуру удаленной установки ОС, мы настоятельно рекомендуем вам ознакомиться с документацией по службе RIS, поставляемой вместе с ОС, документацией TechNet и пакетом Windows Server 2003 Resource Kit.

После установки

После завершения основной установки вы просто определили базовые возможности сервера. Теперь вам необходимо оснастить его пользователями, группами, контроллерами доменов, Active Directory, приложениями, службами и принтерами, как описано в главах 11–18. Но, прежде чем вы соберетесь с духом и перейдете к этим главам, мы хотели бы рассмотреть еще два вопроса.

Активизация

Пытаясь обуздать распространение пиратского ПО, Microsoft реализовала функцию контроля за инсталляцией, получившую название *активизации (Activation)* (которая впервые появилась в Windows XP). После первоначальной установки продукта, такого как Windows Server 2003, Microsoft предоставляет вам 30-дневный период, в течение которого вы должны связаться с ней и активизировать продукт. Если вы проигнорируете активизацию продукта, на 31-й день он перестанет функционировать. Единственное действие, которое вы сможете выполнять с этого момента, — это активизация. После активизации продукт станет нормально функционировать.

Процесс активизации требует, чтобы для вашей компьютерной системы был сгенерирован 50-разрядный код. Этот код является уникальным для вашей системы и используется для связывания кода вашего продукта с компьютерной системой. Если какой-либо другой компьютер попытается активизировать тот же код продукта на другом компьютере, Microsoft решит, что вы используете ее ПО пиратским способом или, по меньшей мере, пытаетесь установить его на другой системе, не приобретая другой пакет. В основе процесса активизации лежит этот идентификатор компьютера, который генерируется соединением уникальных идентификаторов 10-ти различных частей вашего компьютера, включая материнскую плату, ЦП и жесткие диски. Если вы смените шесть из этих частей, система решит, что вы сменили компьютер и ваше состояние активизации должно быть прекращено. Вы должны вновь связаться с Microsoft и объяснить, что вы только обновили свою существующую систему и что вы только что не установили продукт на полностью новую вторую систему. Вы можете представить себе большую головную боль?

Активизацию можно осуществлять посредством Internet, в этом случае она занимает всего несколько секунд. Активизацию можно также осуществлять по телефону, посредством которого вы должны сообщить представителю клиентской службы 50-разрядный идентификатор вашего компьютера, а он, в свою очередь, должен сообщить вам длинный ключ подтверждения, который вам следует ввести.

Для активизации системы вы можете щелкнуть на всплывающем "пузырьке" напоминания, который появляется в *области уведомления (notification area)* (ранее), известной как *лоток пиктограмм (icon tray)* или *системный лоток (system tray)*, который располагается рядом с пиктограммой часов. До тех пор пока вы не выполните активизацию, операционная

система будет напоминать вам о ней ежедневно или при каждом входе в систему. Процесс активизации можно также инициировать с помощью запуска мастер-программы активизации (Activation Wizard), которую можно обнаружить в меню Start. Вначале она появляется в меню верхнего уровня, а после активизации — только в разделе All Programs⇨Accessories⇨ System Tools (Программы⇨Стандартные⇨Служебные).

Пакеты обновления Windows 2003

Пакет обновления (service pack) — это версия обновлений или "заплаток" для программного продукта. Microsoft известна своими версиями пакетов обновления для исправления своего ПО. Это подтверждает тот факт, что Microsoft в достаточной мере заботится о своих пользователях с точки зрения сопровождения продукта, но не проявляет достаточной заботы о том, чтобы сразу предоставить им надежно работающий продукт. Если все пойдет как обычно, то служебный пакет Windows 2003 будет выпущен примерно через три месяца после выпуска Windows Server 2003.

Чтобы облегчить бремя поддержания самой последней версии, Microsoft добавила в Windows Server 2003 две возможности. Во-первых, конфигурация инструмента Windows Update может быть настроена таким образом, чтобы регулярно проверять наличие новых обновлений и предлагать вам загрузить и установить их. Во-вторых, служебные пакеты могут быть помещены сразу же за файлами дистрибуции, так что начальная установка завершается автоматическим применением служебных пакетов. Другими словами, служебные пакеты могут применяться в момент дистрибуции, так что новая система автоматически получает установку, на которую наложены служебные пакеты. После того как служебные пакеты для Windows 2003 станут доступны, вы можете прочесть сопроводительную документацию и точно узнать, как поменять их в одном потоке с установкой.

Служебные пакеты Windows 2003 не завлекут вас в ловушку, связанную с необходимостью установки файлов с исходного дистрибутивного компакт-диска после применения служебного пакета. Другими словами, добавление новых служб не требует повторного применения служебных пакетов, а применение служебных пакетов не требует повторной установки служб с дистрибутивного компакт-диска.

Microsoft рекламирует выпуски служебных пакетов, что облегчает пользователям находить, загружать и применять эти "сокровища". И как всегда, у вас под рукой ссылка на Web-страницу, посвященную нашему конкретному продукту: `www.microsoft.com/windowserver2003/`.

Автоматическое восстановление системы

Автоматическое восстановление системы (Automated System Recovery — ASR) частично предназначено для замены функций прежнего процесса восстановления ERD (Emergency Repair Disk), который вы, возможно, помните по Windows NT. Функцию ASR можно использовать для возврата к сохраненным параметрам конфигурации системы в случае ее полного отказа. Единственным недостатком функции ASR является то, что она восстанавливает файлы, обнаруженные только в системном разделе. Поэтому, если вы храните приложения или файлы пользовательских данных в других разделах, ASR не предложит вам мер, гарантирующих сохранность этих элементов.

Для использования восстановления ASR вы должны создать набор резервирования. Для создания набора резервирования ASR необходимо открыть вкладку Welcome (Добро пожаловать) утилиты Backup (Архивация данных) (Start⇨AllPrograms⇨Accessories⇨System Tools⇨Backup). Набор резервирования ASR состоит из одного флоппи-диска и одной или нескольких резервных лент (в зависимости от объема данных, хранимых в вашем системном разделе). Для восстановления отказавшей системы вы должны выполнить начальную загрузку

исходной программы установки либо с загрузочного компакт-диска, либо с использованием загрузочной инсталляционной дискеты, а затем, после того, как вам будет предложено инициировать процесс восстановления ASR, нажать клавишу <F2>. Затем вы получите приглашение использовать флоппи-диск и ваши резервные ленты.

Если вы желаете защитить все ваши данные, у вас есть две возможности. Вы можете воспользоваться полным набором функций резервного копирования "родной" утилиты Backup (которые включают сохранение состояния системы). Либо вы можете потратить деньги на качественное решение по резервному копированию от независимого поставщика, которое предлагает восстановление с ленты после простой начальной загрузки с флоппи-диска вместо требования полной переустановки ОС для выполнения восстановления.

Ой, MOSL установка не пошла/

В большинстве случаев, если ваше оборудование входит в перечень HCL (Hardware Compatibility List — список совместимого оборудования), установка по легкости напоминает легкий дождичек. (А как на счет не прекращающегося ливня?) Для этих остальных случаев мы приводим перечень распространенных проблем и способы их решения.

- ✓ **Проблемы с компакт-диском.** Полная инсталляция Windows 2003 поставляется на компакт-диске, так что если вы не можете прочитать компакт-диск, вы не сможете установить Windows 2003 (если только вы не выполняете установку по сети, но даже в этом случае с некоторого момента файлы дистрибуции должны быть взяты с компакт-диска). Компакт-диск подобен музыкальным пластинкам или компакт-дискам, одна небольшая царапина или пылинка на поверхности которых может привести к проблемам. С другой стороны, компакт-диск может быть в порядке, но устройство чтения компакт-дисков может работать неправильно, либо Windows 2003 может не распознать устройство. Мы надеемся, что ваше устройство попало в HCL-список. Чтобы определить, исправно ли устройство или компакт-диск, вставьте компакт-диск в другое устройство чтения компакт-дисков и посмотрите, можете ли вы прочитать его на этом устройстве. Определив, какой элемент является источником проблемы, вы можете заменить его и повторить установку.
- ✓ **Проблемы с оборудованием.** Если программа установки Windows 2003 не распознает оборудование сервера, она, вероятнее всего, остановится. Убедитесь в том, что аппаратное обеспечение машины включено в HCL-список и что вы правильно настроили конфигурацию всех устройств. Например, если в вашем распоряжении имеется более одного устройства со SCSI-интерфейсом, убедитесь в том, что они правильно соединены.
- ✓ **"Синий экран смерти".** Иногда программа установки просто заканчивается аварийно и отображает синий экран; в других случаях она отображает коды ошибок, которые может понять только технарь-фанатик. Сам по себе синий экран просто означает, что вы должны перезагрузиться. Однако в результате остановки программы, если вы получили на экране компьютера нечто причудливое, вы можете взглянуть на первые несколько строк, чтобы определить код ошибки, а затем использовать его, чтобы отыскать сообщение об ошибке в соответствующем руководстве. Останов обычно происходит, когда возникают проблемы с драйверами; если вы взглянете чуть дальше первых строк экрана с сообщениями об ошибках, они расскажут вам о том, какие драйверы были загружены на момент аварийной остановки. Неплохо перед перезагрузкой записать первые несколько строк экрана аварийного останова.

- **Проблемы взаимодействия.** Установка машины в существующий домен требует, чтобы новая система была способна взаимодействовать с контроллером домена для создания учетной записи компьютера домена. Если взаимодействие по каким-то причинам невозможно (например, из-за неподходящего сетевого адаптера, неверно выбранного драйвера, испорченного или неустановленного кабеля, отключенного контроллера домена или слишком высокого сетевого трафика), вы не сможете присоединиться к домену. В некоторых случаях вы можете решить проблему быстро, заменив кабель либо дав возможность системе попытаться установить соединение во второй или в третий раз. В других случаях вы можете отложить противостояние с проблемой, присоединившись к рабочей группе, а не к домену. Затем, уже имея в своем распоряжении функционирующую систему, вы можете решить любую проблему (с адаптером, драйвером и проблемы конфигурации).
- **Проблемы зависимостей.** Работа некоторых служб Windows 2003 зависит от того, корректно ли загружены некоторые службы. Если служба А не загружается, служба В не работает, и вы получите сообщение об ошибке, если служба В настроена на автоматический запуск при загрузке службы А. Например, если сетевой адаптер установлен неверно, всем службам, которые используют его, не удастся стартовать. Так что ваше первоочередное дело — заставить адаптер нормально работать. Если вы столкнулись с подобной проблемой, пройдя значительный путь в процессе установки, вы можете посмотреть журнал ошибок (Start⇨Administrative Tools⇨Event Viewer (Пуск⇨Администрирование⇨Просмотр событий)), чтобы определить, какая служба не стартовала, и начать отрабатывать проблему с этого места.
- **Ошибки файла сценариев.** Программа автоматической установки Windows 2003 (описанная в следующем разделе) "не прощает", если вы неправильно ввели сценарий. Если сценарий останавливается посредине и программа установки Windows 2003 просит вас ввести что-то вручную, значит, вы ошиблись при вводе сценария. Проверьте входной файл на предмет перестановки букв или других ошибок. Сценарий предполагает точное выполнение компьютером всех инструкций, введенных в него. Если вы введете неверную информацию, программа установки не получит ожидаемой информации.

- **Файлы SERVER1.TXT-SERVER4.TXT.** Если вы обнаружили проблемы с драйверами или другие проблемы, отсутствующие в предыдущем перечне, получите и прочтите эти файлы, чтобы понять, не повлияли ли на вашу установку какие-то новшества от Microsoft, которые не попали в руководства. Эти файлы расположены в подкаталоге \docs.

Об автоматической установке

Возможность автоматической установки позволяет вам установить Windows 2003 без применения клавиатуры. Просто запустите процесс и идите по своим делам. Автоматическая установка использует файл сценариев, который извлекает информацию и нажатия клавиш из заранее составленного вами файла данных. Если вы уже знаете ответы на все вопросы, которые задает программа инсталляции, вы можете ответить на них и поместить ответы в файл данных. Для различных типов установки вы можете использовать разные файлы данных.

Автоматическая установка удобна для организаций, которые устанавливают Windows 2003 на огромном количестве машин с одинаковой конфигурацией оборудования. Крупные сети предприятий, которые включают удаленные офисы, также могут выиграть от автоматической установки, поскольку администраторы головного офиса могут настроить файлы сценариев и передать их в удаленные офисы. При этом мы хотели бы предупредить вас о необходимости тщательно проверить точность сценариев в головном офисе; в противном случае персонал удаленных офисов может вскоре взмолиться о помощи!

Подробности, касающиеся автоматической установки, можно найти в документации Windows Server 2003 Resource Kit.

Глава 10

Выходим в мир!

В этой главе...

- Настройка конфигурации сервера
- Конфигурирование контроллеров доменов
- Роли сервера
- Использование удаленного доступа

Даже после того как вы установите Windows Server 2003, вы по-прежнему будете сталкиваться с необходимостью принимать многочисленные решения, прежде чем сможете с облегчением сказать: "Миссия выполнена!" Какая роль отводится серверу в сети? Будет ли он ведущим звеном многочисленных сетевых интерфейсов? Потребуется ли вам удаленный доступ? В этой главе вы получите ответы на эти вопросы и узнаете, что можно предпринять для реализации своих решений.

Прежде чем вы начнете действовать, мы хотим предупредить вас, что некоторые темы, предложенные в этой главе, — предельно сложны- Мы стараемся дать общий обзор каждой темы, но в некоторых случаях отдельные вопросы выходят за рамки данной книги. В подобных ситуациях мы рекомендуем обратиться к другим источникам и материалам, в которых вы сможете найти ясное и заслуживающее доверия изложение этих тем.

Мастер конфигурирования сервера

В этом разделе подробно описывается процедура, которую необходимо выполнить, чтобы заставить ваш сервер Windows Server 2003 "встать на ноги" и заработать. Когда вы в первый раз войдете в систему Windows Server 2003 после завершения начальной установки, вы столкнетесь с мастер-программой настройки конфигурации сервера — Configure Your Server Wizard. Этот мастер появляется по умолчанию при первом входе в систему. Вновь получить к нему доступ можно с помощью команды Start⇨All Programs⇨Administrative Tools⇨Configure Your Server (Пуск⇨Программы⇨Администрирование⇨Конфигурация вашего сервера).

Этот мастер выглядит и работает совершенно иначе, чем мастер настройки конфигурации в системе Windows 2000. Если вы привыкли к среде Windows 2000, приготовьтесь к некоторой доле новизны.

Щелкните на кнопке Next страницы Welcome мастера Configure Your Server Wizard, чтобы перейти на страницу Preliminary Steps (Предварительные шаги). Страница Preliminary Steps информирует вас о том, что должен иметь ваш компьютер,

- ✓ Сетевое соединение.
- ✓ Соединение с Internet.
- ✓ Периферийные устройства (принтеры, внешние диски), которые правильно подключены и функционируют.
- ✓ Доступные дистрибутивные файлы для Windows Server 2003 (или весь компакт-диск).

Если вы можете принять эти условия, щелкните на кнопке Next.

Вы можете использовать страницу Server Role (Роль сервера), показанную на рис. 10.1, для установки широкого набора сетевых служб, в том числе следующих.

- ✓ DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации узлов) — см. главу 14.
- ✓ DNS (Domain Name Service — служба имен доменов) — см. главу 14.
- ✓ Active Directory — см. главы 11 и 12,
- ✓ Файловые службы — см. главу 16,
- ✓ Службы печати — см. главу 13.
- ✓ Служба удаленного доступа — рассматривается в этой главе.
- ✓ IIS (Internet Information Services — информационные службы Internet) — рассматривается в этой главе.
- ✓ WINS (Windows Internet Naming Service — служба имен Internet для Windows) — см. главу 14.

Так же как и в случае более развитых служб, например Terminal Service, сервер Streaming Media Server, служба SharePoint Team Services и сервер Real Time Communication Server, вам необходимо обратиться к документации, такой как Resource Kit для Windows Server 2003.

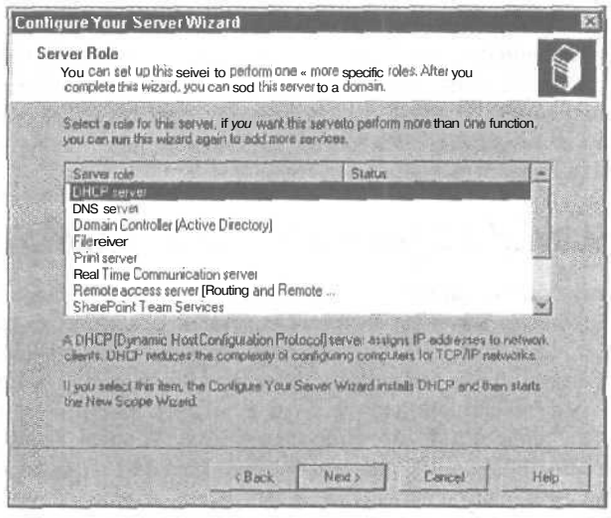


Рис. 10.1. Диалоговое окно выбора роли сервера

Посадка вашего первого леса

Чтобы подготовить и запустить сервер, вам в первую очередь необходимо знать, является ли этот сервер первым в вашем домене. Если это первый сервер, то утилита Configure Your Server Wizard поможет вам установить базовые службы, необходимые для поддержки домена. Если это не первый сервер в сети, вы можете установить сервер в качестве еще одного контролера домена или просто в качестве рядового сервера домена. Вы можете также назначить сервер в качестве автономного.

Если вы устанавливаете первый контроллер домена в первом домене для всей вашей организации, вы устанавливаете больше, чем просто домен; вы также определяете корень вашего первого дерева и корень вашего первого леса. В терминологии доменов Active Directory группа компьютеров, которая совместно использует пространство имен и структуру DNS, называется *доменом (domain)*. Группа доменов, связанная отношениями "родитель-потомок" (также аналогично корням дерева), называется *деревом (tree)*. Дерево доменов — это набор доменов, связанных транзитивными двусторонними доверительными отношениями, разделяющих общую схему, конфигурацию и глобальный каталог. Домены также образуют непрерывное иерархическое пространство имен с одним из доменов, который представляет собой корень доменов.

Первый домен, установленный в дереве, рассматривается как *корневой домен* дерева. Он может рассматриваться как корневой домен леса только в том случае, если он является первым доменом леса, что обсуждается далее.

Группа деревьев связана между собой как лес. Способность организовывать сети в сложные логические структуры пространства имен обеспечивает Windows 2003 (и Windows Server 2000) масштабируемость и гибкость в качестве корпоративной сетевой операционной системы.

Лес (forest) — это один или более доменов, разделяющих общую схему, конфигурацию и глобальный каталог. Лес может обладать или не обладать общим пространством имен доменов. Если лес состоит из одного дерева, он будет обладать общим пространством имен доменов, так как он — всего лишь дерево. Поскольку лес может включать более одного дерева доменов (это не требование, это просто допустимо), эти различные деревья доменов обладают своими собственными непрерывными пространствами имен.

Все домены внутри дерева доменов и все деревья внутри одного леса пользуются преимуществами соединения, обладающего свойствами транзитивного двустороннего доверительного отношения, которое по умолчанию представляет собой доверительное отношение между доменами Windows 2003 и Windows 2000. Транзитивное двустороннее доверительное отношение является комбинацией транзитивного доверительного отношения и двустороннего доверительного отношения. Это полное доверие между всеми доменами в иерархии доменов Active Directory помогает сформировать лес как единый узел посредством общей схемы, конфигурации и глобального каталога.

Первый домен Windows Server 2003 и Windows Server 2003, установленный в лесу, рассматривается как *корневой домен леса (forest root domain)*.

Первый созданный вами контроллер домена также определяет домен. Если это первый домен в вашей сети, он также является корнем первого дерева и первым деревом в лесу. Более подробную информацию о логической структуре доменов, деревьев и лесов вы можете найти в пакете Windows Server 2003 Resource Kit.

А теперь предположим, что ваш сервер — первый сервер в сети. Для настройки сервера выполните следующие действия.

1. **Щелкните на кнопке Next диалогового окна Configure Your Server Wizard. Затем щелкните на кнопке Next страницы Preliminary Steps.**

Диалоговое окно мастер-программы Configure Your Server Wizard появляется автоматически, когда вы в первый раз входите в систему Windows Server 2003. Если оно еще не открыто, запустите программу из меню Start с помощью команды Start⇨All Programs⇨Administrative Tools⇨Configure Your Server.

2. **Выберите опцию Domain Controller (Active Directory) (Контроллер домена (Active Directory)), а затем щелкните на кнопке Next.**

На экране отображается сводка проводимых изменений.

3. **Щелкните на кнопке Finish (Готово).**

   Запустится мастер-программа Active Directory Installation Wizard.

   В ходе настройки конфигурации мастер-программа может предложить вам установить дистрибутивный компакт-диск. В этом случае поместите компакт-диск в локальное устройство чтения компакт-дисков или укажите путь к локальной или сетевой копии файлов дистрибуции.

4. **Щелкните на кнопке Next.**

   На экране отобразится страница Domain Controller Type (Тип контроллера домена).

5. **Предполагая, что это первый контроллер домена в вашем новом домене, выберите опцию Domain Controller for a New Domain (Контроллер домена для нового домена). Щелкните на кнопке Next.**

   Отобразится страница Create New Domain (Создать новый домен).

6. **Предполагая, что это первый домен в новом лесу (что означает также, что это новое дерево), выберите опцию Domain in a New Forest (Домен в новом лесу). Щелкните на кнопке Next.**

   Появится страница New Domain Name (Новое имя домена).

7. **Введите имя нового домена.**

   Имя должно быть представлено в формате FQDN (fully qualified domain name — полностью определенное имя домена), например `mycompany.local` или `googleplex.com`. Это не имя вашего сервера; его вы определили при первой установке Windows Server 2003. Это имя домена верхнего уровня.

   В качестве имени домена вы можете использовать то же имя, которое будет использоваться в Internet для доступа вашей организации (например, `googleplex.com`), либо можете использовать внутреннее доменное имя, которое не будет связано с Internet (например, mycompany. local или mycompany. ad)

8. **Щелкните на кнопке Next.**

   Появится страница NetBIOS Domain Name с автоматически сгенерированным именем домена. Это имя используют системы и приложения, несовместимые с пакетом Active Directory. В большинстве случаев это имя просто представляет первые 15 символов, предшествующих первой точке вашего доменного имени, наподобие такого, как `googleplex` или mycompany.

9. **Если предлагаемое имя подходит (обычно так и есть), щелкните на кнопке Next В противном случае дайте другое имя и щелкните на этой же кнопке.**

   Единственное ограничение, накладываемое на NetBIOS-имя домена, заключается в том, что оно не должно превышать 15 символов, состоять только из принятых для систем NetBIOS и DNS символов (*Aa-Zz*, 1–9 и дефис) и быть уникальным в рамках домена, в котором оно находится.

   На экране появится страница Database and Log Folder (База данных и папка журнала), содержащая запрос о пути к папкам-хранилищам для главного каталога и файлов журнала. Определение путей к жестким дискам, отличных от того, который хранит системный раздел, повышает общую производительность, однако в большинстве случаев достаточно принять путь, предполагаемый по умолчанию.

10. **Щелкните на кнопке Next.**

    Появится страница Shared System Volume (Общий системный том), которая содержит запрос пути для хранения папки SYSVOL. Эту папку можно расположить на отдельном жестком диске либо принять путь, предполагаемый по умолчанию.

11. **Щелкните на кнопке Next.**

    Если вы не установили службу DNS, появится страница DNS Registration Diagnostics (Регистрационная диагностика DNS). Это указывает на обнаружение сервера DNS, настроенного на обслуживание новой зоны, создаваемой для нового домена.

12. **Выберите опцию Install and Configure DNS Server on this Computer (Установить и сконфигурировать DNS-сервер на этом компьютере), а затем щелкните на кнопке Next.**

    Появится страница Permissions (Разрешения), и вам предлагается решить, будут ли использоваться разрешения, принятые в системах, предшествующих Windows 2000. В большинстве случаев использовать разрешения, совместимые с серверами, предшествующими Windows 2000, стоит только в тех случаях, когда вы уверены, что будете использовать в домене унаследованные системы, например Windows *9x* или Windows NT Workstation, поскольку это влияет на безопасность домена, а возможно, и леса.

    При выборе варианта с использованием разрешений, совместимых с системами-предшественницами ОС Windows 2000 Server, вы позволяете мастер-программе Active Directory Installation Wizard настроить конфигурацию домена (а возможно, и леса, если эта установка — первая в лесу), так что к группе Compatible Access (Совместимый доступ) добавляются группы Anonymous Logon (Анонимный вход в систему) и Everyone security (Безопасность для каждого).

    Если вы не желаете, чтобы группе Anonymous Logon домена было разрешено чтение пользовательской и групповой информации, и в домене отсутствуют клиенты устаревших систем, вы должны выбрать опцию Permissions compatible only with Windows Server 2003 Operating System (Разрешения совместимы только с операционной системой Windows Server 2003).

13. **Выберите требуемую опцию для предпочтительного типа разрешений, а затем щелкните на кнопке Next.**

    Появится страница Directory Services Restore Mode Administrator Password (Пароль администратора режима восстановления служб каталогов), содержащая запрос на ввод уникального пароля, который используется для входа в систему в режиме восстановления служб каталогов, если отказ системы требует восстановления Active Directory.

14. **Введите пароль и щелкните на кнопке Next.**

    Появится страница Summary (Сводка), в которой перечислены изменения, вносимые в систему.

15. **Щелкните на кнопке Next.**

    Процесс установки и настройки конфигурации занимает значительное время (в некоторых системах — до одного часа), так что наберитесь терпения.

16. **Если ваша система использует IP-адрес, динамически или автоматически присвоенный службой DHCP, вы можете увидеть всплывающее окно с предупреждением о том, что вам необходимо определить статический IP-адрес для обеспечения надежности службы DNS. Щелкните на кнопке OK в этом диалоговом окне.**

17. **В диалоговом окне Local Area Connection Properties (Подключение по локальной сети: Свойства) выберите переключатель Internet Protocol (TCP/IP), а затем щелкните на кнопке Properties.**

    Появится диалоговое окно Internet Protocol (TCP/IP) Properties.

18. **Выберите опцию Use the Following IP Address (Использовать следующий IP-адрес). Введите в поля IP Address и Subnet Mask предпочтительные параметры и щелкните на кнопке OK.**

    Если вы не знаете, какой IP-адрес назначить, используйте следующие: 192.168.0.1 и 255.255.255.0. Чтобы узнать больше об управлении, назначении и конфигурировании протокола TCP/IP, обратитесь к главе 14.

19. **Чтобы закрыть диалоговое окно Local Area Connection Properties, щелкните на кнопке Close (Закрыть).**

20. **После того как отобразится сообщение о завершении установки, щелкните на кнопке Finish.**

21. **После того как вам будет предложено перезагрузить систему, щелкните на кнопке Restart Now (Перезагрузить систему).**

22. **После перезагрузки системы вновь войдите в нее. Итак, вы завершили настройку конфигурации!**

Теперь вы можете решить, какие сетевые или прикладные компоненты вы желаете установить на своем новом сервере. Второй, третий и четвертый серверы, устанавливаемые в сети, могут исполнять различные сетевые роли, в том числе следующие.

- ✓ Рядовой контроллер домена, обеспечивающего работу Active Directory.
- ✓ Сетевой управляющий сервер, обеспечивающий работу служб DHCP, DNS, WINS, маршрутизации и удаленного доступа, а также многих других сетевых служб.
- ✓ Файловый сервер или сервер печати.
- ✓ Web-сервер, мультимедиа-сервер или сервер приложений.

Active Directory мы рассмотрим в главах 11 и 12, файл-серверы — в главе 16, а серверы печати — в главе 13. Все, что вам необходимо знать о возможностях конфигурирования вашего сервера, изложено в этой главе.

Windows Server 2003 — просто автономная система, которая функционирует подобно рабочей станции до тех пор, пока вы не воспользуетесь конфигурацией, предлагаемой утилитой Configure Your Server Wizard. После этого ваша машина с Windows Server 2003 может выполнять практически любые действия, которые вы пожелаете. В отличие от системы Windows NT, в которой вы должны назначить либо основной, либо резервный контроллер, все контроллеры доменов в системах под управлением Windows Server 2003, по существу, равны. Любой из контроллеров домена разделяет ответственность за поддержку домена, обновление Active Directory и управляет распределением прав доступа и сетевой нагрузки.

Подготовка средств общения

Windows Server 2003 включает Internet Information Services (IIS) 6.0 и поддерживает потоковый сервер мультимедиа (Streaming Media Server), также известный как служба мультимедиа Windows (Windows Media Services — WMS). Сервер IIS позволяет организовать Web- и FTP-узлы для пользователей интрасетей и Internet. С помощью WMS вы можете создать сногсшибательные мультимедиа-презентации, сочетающие аудио, видео, слайды, интерактивное мультимедиа и многие другие возможности, обеспечиваемые за счет потокового соединения.

Вы можете воспользоваться элементами IIS и WMS утилиты Configure Your Server Wizard, чтобы непосредственно перейти к средствам администрирования для IIS 6.0 и WMS. Вы можете также получить доступ к утилите Internet Information Services Manager, диалоговое окно которой показано на рис. 10.2, с помощью команды Start⇨Administrative Tools⇨Internet Information Services (IIS) Manager. (Эта утилита известна также как встроенная консоль MMC (консоль управления Microsoft — Microsoft Management Console).)

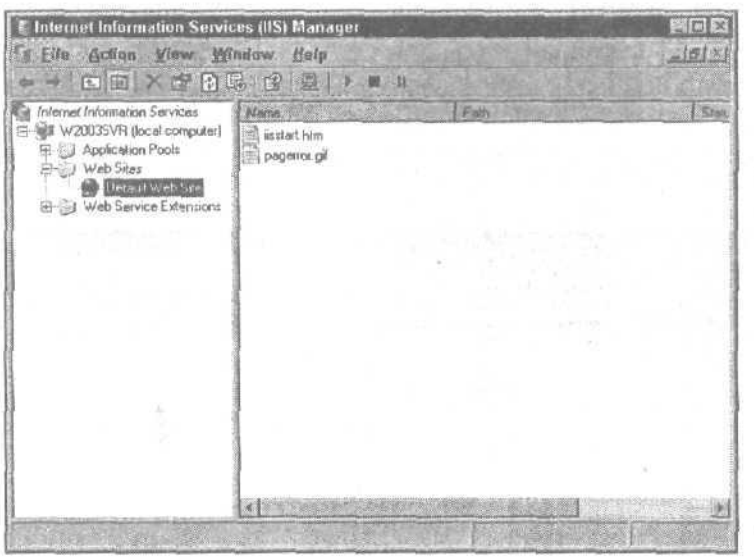


Рис. 10.2. Утилита Internet Information Services Manager для IIS версии 6.0

Чтобы возложить на сервер Windows Server 2003 функции службы Windows Media Services, сначала сконфигурируйте его как потоковый мультимедиа-сервер с помощью команды Start⇨Administrative Tools⇨Configure Your Server Wizard. Затем присвойте серверу роль Streaming media server, которая позволит вам завершить его установку и передавать содержимое аудио- и видеофайлов клиентам посредством Internet или интрасети вашей компании.

Сервер US 6.0 — сам хозяин своих приложений, и его функции не описываются в этой книге. Если вы желаете установить эту службу на своем сервере, обратитесь к комплектам Windows Server 2003 Resource Kit или руководству TechNet.

Налаживание соседских отношений

Функция Networking (Сеть) утилиты Configure Your Server Wizard обеспечивает возможность быстрого доступа к средствам настройки конфигурации, которые используются для управления службами DHCP, DNS, Routing and Remote Access. *DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации узла)* — это метод автоматической

настройки параметров TCP/IP для клиентов и не критичных для работы сети серверов, осуществляемой при начальном запуске системы. *DNS (Domain Name System — служба имен доменов)* — метод разрешения имен узлов в IP-адреса. Службы DHCP и DNS рассматриваются в главе 14.

Службы DHCP и DNS — это чрезвычайно сложные темы, которые заслуживают отдельного рассмотрения, однако в настоящей книге они подробно не рассматриваются. Исчерпывающие инструкции по настройке конфигурации и управлению этими службами можно найти в комплекте Windows Service 2003 Resource Kit.

Служба маршрутизации и удаленного доступа (Routing and Remote Access Service — RRAS) выполняет две функции: маршрутизацию и удаленный доступ (кто бы мог подумать!). Маршрутизация — это средство адресации сетевых сообщений в локальной сети или (при помощи каналов удаленного доступа) в рамках глобальной сети. Удаленный доступ — это средство установления сетевых соединений по обычным телефонным линиям или по цифровым телефонным линиям ISDN (Integrated Services Digital Network — цифровая сеть с комплексными услугами). Windows Server 2003 может функционировать как клиент, если установлено соединение с удаленными системами, или работать в качестве сервера при приеме входящих вызовов. Выбор узла Routing and Remote Access области Networking утилиты Configure Your Server Wizard позволяет запустить консоль управления Routing and Remote Access (рис. 10.3). С помощью этой консоли вы можете установить и настроить конфигурацию службы Routing and Remote Access.

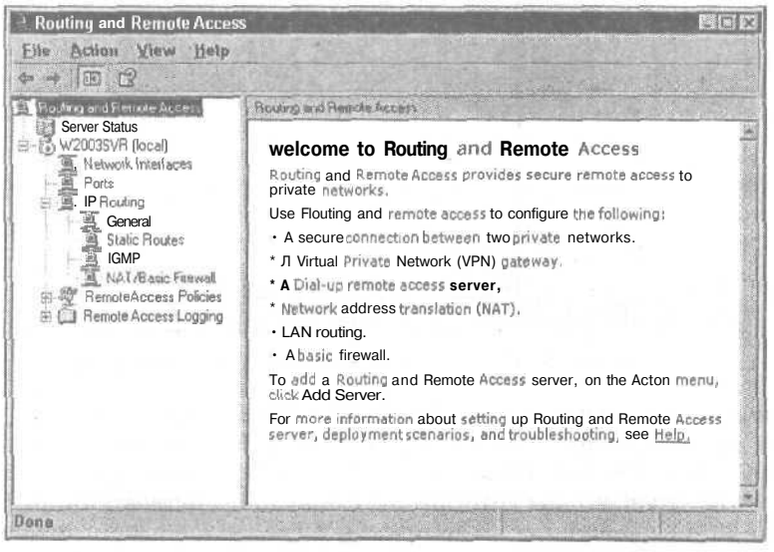


Рис. 10.3. Консоль управления ***Routing and Remote Access***

Ниже приводятся основные шаги по настройке этой службы.

1. **Откройте окно консоли управления Routing and Remote Access (Start⇨Administrative Tools⇨Routing and Remote Access).**
2. **Щелкните на элементе Routing and Remote Access в левой панели.**
   Отобразится список серверов сети.

3. **Щелкните правой кнопкой мыши на элементе, соответствующем вашему серверу, и выберите опцию Configure and Enable Routing and Remote Access (Сконфигурировать и включить маршрутизацию и удаленный доступ).**

   Появится окно мастер-программы установки сервера маршрутизации и удаленного доступа — Routing and Remote Access Server Setup Wizard.

4. **Щелкните на кнопке Next.**

   Мастер предоставит вам список альтернатив для стандартных конфигураций и возможность установки параметров вручную. В окнах Common Configurations (Стандартные конфигурации) доступны следующие опции.

   - Remote Access (dial-up or VPN) (Удаленный доступ (коммутируемый или VPN).
   - Network address translation (NAT) (Трансляция сетевых адресов).
   - Virtual private network (VPN) access and NAT (Доступ к виртуальной частной сети и NAT).
   - Secure connection between two private networks (Безопасное соединение двух частных сетей).
   - Custom configuration (Пользовательская конфигурация).

5. **Выберите вариант, который в наибольшей мере отвечает вашим потребностям, или выберите опцию Custom configuration и установите необходимые параметры вручную.**

6. **Щелкните на кнопке Next.**

   Каждая из четырех стандартных конфигураций предполагает дальнейшую более тонкую настройку, и мастер-программа установки сервера предложит вам уточнить детали. Более подробную информацию, касающуюся вариантов выбора параметров, можно найти в документации Windows Server 2003 Resource Kit.

7. **Для завершения настройки конфигурации следуйте дальнейшим указаниям утилиты.**

Помните, для того, чтобы включить функцию маршрутизации, вам необходимы по меньшей мере два сетевых интерфейса. Это могут быть сетевые адаптеры, специальные соединения с Internet или модемы.

Хотя кажется, что все необходимые функции включены, мы рекомендуем вам перезагрузить систему, а затем выполнять дальнейшие модификации.

После перезагрузки сервер маршрутизации и удаленного доступа сконфигурирован и функционирует. Все, что теперь необходимо, — это сетевые интерфейсы и еще чуть-чуть настроить конфигурацию. Служба RRAS оснащена GUI-интерфейсом (Graphical User Interface — графический интерфейс пользователя), который является большим шагом вперед по сравнению с предшествующим интерфейсом командной строки с чисто текстовым управлением и отображением. Более того, это средство управления позволяет устанавливать протоколы маршрутизации, интерфейсы мониторов и порты, прослушивать клиентов по коммутируемым линиям, определять правила доступа и модифицировать параметры регистрации. Вам больше никогда не придется использовать команду ROUTE!

Однако маршрутизация — это игра не для робких. По этой причине мы рекомендуем вам обратиться за более подробной информацией к документации Windows Server 2003 Resource Kit Ме желая оставлять вас в полном неведении, мы привели некоторые особенности удаленного доступа в разделе "Другие возможности" далее в этой главе.

Удаленные соединения

Удаленные соединения состоят из двух различных элементов: клиента и сервера. Windows Server 2003 может устанавливать соединение с удаленной системой (как коммутируемый клиент) или принимать входящие соединения от удаленных клиентов (как коммутируемый главный узел). Более подробную информацию об использовании Windows Server 2003 как коммутируемого главного узла можно найти в документации Windows Server 2003 Resource Kit.

Подключаемся к сети

Использование Windows Server 2003 в качестве клиента, работающего с телефонным соединением, не представляется очень трудным. В большинстве случаев вы подключаетесь к поставщику услуг Internet (Internet Service Provider — ISP) для установления Internet-соединения. Мы можем шаг за шагом провести вас через процесс установления подобного соединения, если вы располагаете следующей информацией.

- ✓ Телефонный номер ISP.
- ✓ Регистрационное имя пользователя.
- ✓ Регистрационный пароль пользователя.

Для этого типа подключение мы предполагаем, что у вас имеется модем, а не ISDN-линия иди другое устройство связи. Установить модем вы можете с помощью аплета Add/Remove Hardware (Установка/удаление оборудования) окна Control Panel (Панель управления). Если вы последуете инструкциям, вы удивитесь, насколько легко выполняется установка.

Мы также полагаем, что ваш ISP предлагает простую процедуру регистрации. Если вам требуется ввести в ваше регистрационное имя специальные символы, вы должны досконально изучить меню регистрации или выполнить сценарий регистрации, вам также необходимо обратиться к ISP за инструкциями по конфигурированию Windows Server 2003, чтобы правильно установить соединение.

1. **Для отображения экрана Network Connections (Сетевые подключения) выберите команду Start⇨Settings (Пуск⇨Настройка), как показано на рис. 10.4.**

Чтобы выполнить эти действия, вам требуется установленный модем.

2. **Дважды щелкните на пиктограмме New Connection Wizard (Мастер нового подключения), а затем щелкните на кнопке Next.**
3. **Выберите опцию Connect to the Internet (Подключение к Internet), а затем щелкните на кнопке Next.**
4. **Выберите опцию Connect Using a Dial-up Modem (Подключение с использованием модема), а затем щелкните на кнопке Next.**
5. **Введите имя для этого объекта соединения, такое как ISP-имя, и щелкните на кнопке Next.**
6. **Введите номер телефона и щелкните на кнопке Next**
7. **Выберите опцию, указывающую на то, будет ли этот объект использоваться кем-то другим, кто вошел в эту систему, или только вами, а затем щелкните на кнопке Next.**
8. **Введите регистрационное имя и пароль для учетном записи ISP, а затем щелкните на кнопке Next Щелкните на кнопке Finish (Готово).**

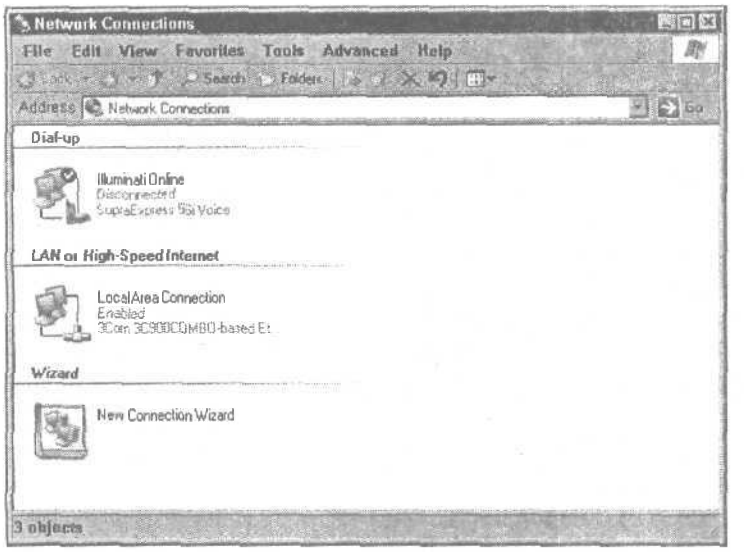


Рис. 10.4. Консоль управления Network Connections (после определения объекта соединения)

Вот оно! Теперь в окне Network Connections появилась пиктограмма с введенным вами именем. Дважды щелкните на пиктограмме, чтобы отобразить диалоговое окно Connection (Подключение). Спустя несколько беспокойных мгновений вы установили соединение и готовы к работе!

Вы можете узнать о состоянии соединения, поместив указатель мыши на пиктограмму соединения (на которой изображены два перекрывающихся компьютера) в системной области (в правом нижнем углу экрана). Вы можете также дважды щелкнуть на пиктограмме для отображения диалогового окна, содержащего более подробную информацию.

Вы можете изменить параметры удаленного соединения, щелкнув правой кнопкой мыши на пиктограмме в окне Network Connections и выбрав вкладку Properties (Свойства). В диалоговом окне для страницы Network Connections Property вы можете изменить любое из свойств соединения.

Чтобы завершить установление соединения, щелкните правой кнопкой мыши на пиктограмме подключения в системной области и выберите опцию Disconnect или дважды щелкните на пиктограмме подключения для отображения окна Details (Подробности), а затем щелкните на кнопке Disconnect.

Другие возможности

Windows Server 2003 включает все последние функциональные возможности, которые можно ожидать от сервера удаленного доступа на основе Windows. Большинство из них знакомы вам по Windows 2000, а некоторые — по Windows XP. Но даже с самыми последними усовершенствованиями Windows Server 2003 сохранила практически все старые возможности и функции. Это значит, что то, чего вы могли достичь с помощью Windows NT или службы RAS Windows 2000, вы еще более эффективно сможете осуществить с использованием службы удаленного доступа Windows Server 2003.

Эти возможности приведены ниже.

- ✓ Протокол PPP' (Point-To-Point Protocol — протокол двухточечного соединения) для исходящих и входящих соединений. Протокол SLIP (Serial Line Internet Protocol — межсетевой протокол для последовательного канала) по-прежнему применяется для исходящих соединений с системами, использующими протокол, отличный от PPP. (ОС Windows XP Professional не поддерживает SLIP для входящих соединений, она может только использовать протокол TCP/IP для соединения посредством SLIP.)
- ✓ Многоканальный протокол PPP для агрегирования аналогичных соединений в рамках одного потока (pipeline).
- ✓ Протокол PPTP (Point-to-Point Tunneling Protocol — туннелируемый протокол PPP) для установления связи поверх Internet для установления безопасного соединения.
- ✓ Шифрование при идентификация для защиты регистрационного пароля.
- ✓ Функции зашиты виртуальных частных сетей (Virtual Private Network — VPN): EPSec и L2TP (за подробностями обратитесь к руководствам Windows Server 2003 Resource Kit или TechNet).
- ✓ Поддержка смарт-карт (которые представляют собой небольшие платы, добавляемые к системе для хранения секретной информации).
- ✓ Полная поддержка службы RADIUS (Remote Authentication Dial-up User Service — служба удаленной идентификации соединения пользователя).
- ✓ Совместно используемые соединения (компьютер использует свое соединение совместно с другими клиентами сети).

Чтобы получить исчерпывающую информацию, касающуюся удаленного доступа, обратитесь к руководству Windows Server 2003 Resource Kit.

Глава 11

Работаем с каталогами

В этой главе...

- Служба каталогов
- Active Directory для Windows Server 2003
- Планирование развертывания Active Directory
- Установка Active Drectory
- Связанные домены

В этой главе вы познакомитесь с обновленным вариантом службы каталогов — Active Directory. Вы узнаете, что такое служба каталогов, почему она необходима для структур Windows типа "домен" или "лес" и как распланировать развертывание и установить Active Directory для Windows Server 2003.

Что такое служба каталогов

На самом деле вы все время пользуетесь службами каталогов, возможно, даже не подозревая об этом. Когда вы голодны и страстно желаете съесть пиццу, вы открываете телефонный каталог и под буквой *П* ищете заведение, где можно заказать эту бесподобную пищу. Этот телефонный справочник — своего рода каталог, содержащий необходимую вам информацию и представляющий способ поиска требуемой информации. (В данном примере — в алфавитном порядке.) Компьютерная служба каталогов во многом аналогична. Она содержит информацию о многочисленных сторонах деятельности вашей кампании, организует информацию и предоставляет в ваше распоряжение средства, которые помогут найти необходимую информацию.

Первой операционной системой от Microsoft, которая предлагала службу каталогов, была Windows 2000. Сетевая ОС NetWare обладает собственной службой каталогов — Novell Directory Services (NDS) или eDirectory для Netware 6 — и предлагалась во всех выпущенных Novell версиях сетевой ОС Network Operating System (NOS) начиная с 1993 года. Microsoft строит всю доменную структуру Windows Server 2003 (которая берет начало в Windows 2000) вокруг служб каталогов, а не просто предлагает ее в качестве надстройки на предыдущие реализации доменов. Служба каталогов Microsoft называется *Active Directory*.

Хотя службы Active Directory и Novell Directory Services не взаимодействуют непосредственно, возможна синхронизация Active Directory с Novell Directory Services посредством служб синхронизации каталогов Microsoft (Microsoft Directory Synchronization Services — MDSS). Службы MDSS, которые включены в число служб для NetWare 5, позволяю синхронизировать Active Directory с NDS и регистрационными базами данных NetWare 3.*x*, так что системные администраторы могут уменьшить общий объем их управленческих задач за счет администрирования одной, а не двух отдельных служб каталогов.

Если говорить о названиях, Microsoft зациклилась на слове *active*. Достаточно вспомнить Active Desktop, Active X, а теперь Active Directory. Тем не менее термин довольно точен — помимо всего прочего, Active Directory действительно активна (если ее правильно использовать).

Знакомство с Active Directory

Для надлежащей работы служба каталогов должна удовлетворять трем основным требованиям.

- ✓ Включать структуру для организации и хранения данных каталога.
- ✓ Обеспечивать средства для формирования запросов и управления данными каталога.
- ✓ Поддерживать метод для поиска данных каталога, а также сеть и ресурсы сервера, которые могли бы соответствовать таким данным. (Например, если данные каталога содержат указатель файла и принтер, служба каталога должна знать, где они расположены и как получить к ним доступ.)

Active Directory для Windows Server 2003 выполняет все эти требования с помощью различных технологий. Более подробно об Active Directory можно узнать в книге Марсией Логри (Marcia Loghry) *Active Directory For Dummies* (выпущенной издательством Wiley Publishing Inc.).

Организация и хранение данных

Структура Active Directory соответствует *протоколу ISO X.500* (ISO означает International Organization for Standardization — Международная организация по стандартизации). На рис. 11.1 показана иерархическая структура каталога X.500. Это общий стандарт, используемый практически во всех службах каталогов, включая не только Active Directory от Microsoft, но также Novell Directory Services (NDS), продукты от Netscape и другие реализации. Протокол X.500 доказал свою полезность для этого вида приложений, поскольку он организует данные иерархически, благодаря чему информация в каталоге представляется в виде набора отдельных хранилищ данных, содержащих сведения о таких структурных единицах, как страны, организационные подразделения, подгруппы и ресурсы. В примере на рис. 11.1 каталог организован в соответствии с пользовательскими объектами.

Сегодня самыми распространенными вариантами стандарта X.500 являются стандарты X.500 1988 и 1993 гг. Версия 1993 года содержит ряд преимуществ по сравнению с более старой версией 1988 года. К счастью, служба каталогов Active Directory для Windows Server 2003 построена именно на версии 1993 года.

Управление данными

Вторую составляющую службы Active Directory обеспечивает специальный протокол, известный как *LDAP (Lightweight Directory Access Protocol — упрощенный протокол доступа к каталогу)*. Протокол LDAP обычно использует в качестве основного соединения порт 389 протокола TCP. Как следует из второй части его названия, протокол LDAP разработан специально для обращения и доступа к данным каталога. (Первая часть его названия — *упрощенный* — объясняется тем фактом, что он представляет собой "облегченную" версию старого, более громоздкого протокола X.500 DAP.)

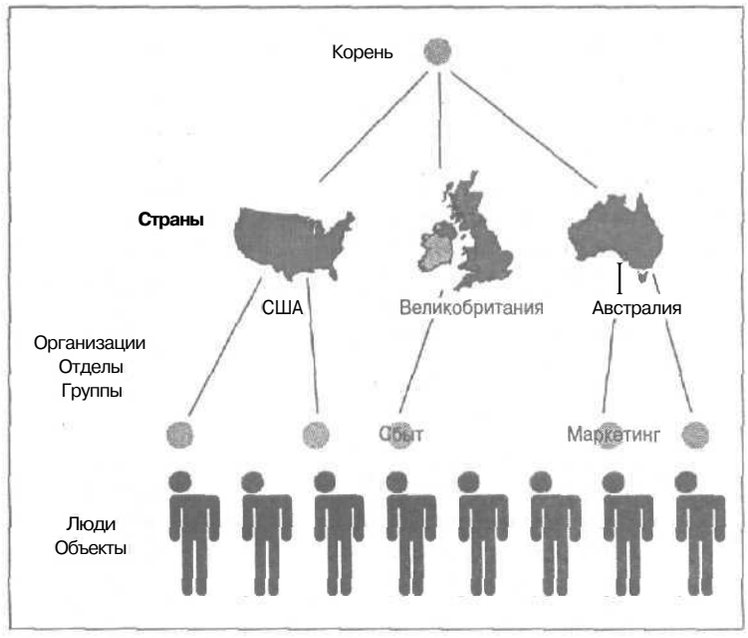


Рис. 11.1. Иерархическая структура каталога X.500

Терминология, используемая в этой главе, будет привычной для тех, кто знаком со службой каталогов сервера Exchange Server компании Microsoft. Это связано с тем, что служба Active Directory сервера Windows Server 2003 использует общее "наследство" (или общую технологию) со службой каталогов Exchange Server. В действительности с Windows Server 2003 поставляется компонент подключения (connector) Exchange Server, чтобы связать две службы каталогов и обмениваться данными между ними. Неудивительно, что этот программный компонент называется *Active Directory Connector*.

Дополнительную информацию, касающуюся протокола LDAP, можно найти на Web-странице RFC#1777 (Request For Comments — запрос на комментарий) по адресу `www.ietf.org/rfc/rfc1777.txt`.

Обнаружение местоположения данных и ресурсов

Поскольку данные каталога Windows Server 2003 структурированы в соответствии с протоколом X.500 и доступ к ним можно получить с помощью протокола LDAP, наверняка должен существовать способ обнаружения местоположения данных каталога. Вот и пришло время третьего недостающего компонента! Каким образом Active Directory удовлетворяет третье и последнее требование к работоспособной службе каталогов? Мы рады вашему вопросу. В основе Active Directory лежит хорошо известный и широко используемый Interaet-стандарт под названием *DNS (Domain Name Service — служба доменных имен*).

О доменах и контроллерах

За каждым большим доменом кроется большой контроллер домена, но прежде чем вы узнаете, как Windows Server 2003 и Windows 2000 используют контроллеры доменов, необходимо кратко напомнить кое-что об использовании Windows NT.

Работа Windows Server 2003 и Windows 2000 с контроллерами доменов существенно отличается от способа работы с доменами Windows NT — в основном благодаря Active Directory. Ну ладно, я не стану снова и снова твердить о том, что и Windows Server 2003, и Windows 2000 поддерживают Active Directory одинаковым способом, так что, то. что вы узнаете здесь о Windows Server 2003, справедливо и в, отношении Windows 2000. (Несколько незначительных отличий, в основном в высокоуровневой схеме контроля и управлении именованием, не описываются в данной книге.)

В начале...

В системе Windows NT 4.0 домены представлялись 15-символьными именами NetBIOS (Network Basic Input Output System — сетевая базовая система ввода-вывода). Подобные домены вращались вокруг единственной базы данных пользователя/группы/правил, которая называлась базой данных SAM (Security Account Manager — администратор учетных данных в системе защиты) и хранилась в формате с перезаписью на единственном основном сервере, известном как *основной контроллер домена (primary domain controller — PDC)*.

Имена NetBIOS могут состоять из 16 символов. В операционных системах от Microsoft имена NetBIOS ограничены 15 символами; 16 символ скрыт и используется как суффикс NetBIOS сетевым ПО Microsoft для идентификации служб, установленных в данной системе. Дополнительную информацию о суффиксах NetBIOS в среде Microsoft можно найти на Web-странице по адресу `http://support.microsoft.com/default.aspx?scid=KB;en-us;q163409`.

Доступ к базе данных домена требуется для доступа к ресурсам домена, так что любая модель, которая зависит от единственного контроллера домена, служит потенциальным источником отказа. Для повышения уровня готовности и надежности базы данных домена Microsoft добавила в комплект второй тип сервера, известный как *BDC (backup domain controller — резервный контроллер домена)*, который хранит только версию базы данных SAM "только для чтения". Пользователи могут получить доступ к BCD для регистрации в домене и получения информации о пользователях, группах или учетной информации, однако изменения в базу данных можно вносить только через PDC.

В данном типе доменной среды для поддержания синхронности контроллер PDC должен периодически обновлять базу данных SAM на всех контроллерах BDC в своем домене. Даже в случае отказа PDC-контроллера, можно перевести BDC-контроллер в разряд PDC-контроллеров и разрешить запись в его базу данных SAM. Однако PDC- и BDC-контроллеры связаны неразрывным отношением "главный-подчиненный", поскольку изменения, внесенные в базу данных SAM, должны применяться к контроллеру PDC и копироваться с PDC на все контроллеры BDC. Таким образом, если PDC-контроллер отказывает, в базу данных SAM нельзя внести никаких изменений до тех пор, пока PDC не будет восстановлен или BDC не будет присвоен статус нового PDC. Вы все усвоили?

Хотя это выглядит как форма подчинения, отношение главный–подчиненный на компьютерном языке означает следующее: "все изменения, которые происходят на "главном", копируются на все "подчиненные", и "только "главный" может принимать изменения и копировать на подчиненные".

Сервер Windows Server 2003 больше не использует имена NetBIOS для именования своих доменов; вместо этого он использует имена доменов DNS. (Более подробно об именах DNS-доменов рассказывается в главе 14.) Например, вместо имени домена Dummies вы можете в качестве допустимого имени использовать `sales.dummies.com`. Однако вы по-прежнему можете использовать имена NetBIOS для обращения к доменам, что является требованием всех систем, не поддерживающих Active Directory, таких как клиентские ОС Windows 98 и Windows NT, которые иногда называют унаследованными клиентами. (Вот почему вы определяете подобное имя при установке Active Directory, как описано в главе 10.) Аналогично, концепция подсистемы SAM больше не используется в доменах Windows Server 2003. Вся информация о пользователях, паролях и группах хранится в Active Directory. Поэтому вместо серверов, которые могут считывать записывать данные в базу SAM, серверы могут предоставить услуги протокола LDAP, которые необходимы для взаимодействия с Active Directory.

В сетях под управлением Windows Server 2003 серверы, которые управляют службой протокола LDAP, являются контроллерами домена. Так же как в сетях на основе Windows NT, эти серверы отвечают за идентификацию и другие виды деятельности в рамках домена. Однако в сетях Windows Server 2003 серверы используют Active Directory для предоставления услуг, которые их устаревшие двойники обеспечивали с помощью базы данных SAM.

К чему все эти ухищрения

Концепция PDC- и BDC-контроллеров не используется в структуре домена Active Directory для Windows 2000 и Windows Server 2003. В этом чудесном новом мире все контроллеры доменов равны (хотя, конечно, некоторые "более равны", чем другие). Как же удается поддерживать это равенство? Процесс, известный как *тиражирование с несколькими хозяевами операций (multi-master replication)*, обеспечивает распространение изменений, произошедших в одном из котроллеров домена, на все остальные контроллеры этого домена. Таким образом, вместо прежних отношений "главный-подчиненный" между контроллерами PDC и BDC имеют место равноправные отношения между всеми контроллерами домена Windows Server 2003 (и за его пределами) при наличии доверительных отношений. (*Доверительные отношения (trust relationship)* — специальный порядок доступа между доменами, который вы определяете, когда пользователям одного домена требуется доступ к ресурсам другого домена.)

Поскольку вы можете быть не в состоянии заменить все ваши контроллеры доменов Windows NT 4.0 на Windows Server 2003 одним "лихим кавалерийским наскоком", Windows Server 2003 позволяет вам эксплуатировать ваши домены в *смешанном* режиме. Это дает возможность контроллерам BDC Windows NT 4.0 (но не PDC) участвовать в работе доменов Windows Server 2003. Идея состоит в том, что вы начинаете с замены PDC-контроллеров Windows NT 4.0 на Windows Server 2003 и затем переходите на другую серверную систему в масштабах всего предприятия. Зачастую сюда включается модернизация или полный демонтаж всех существующих серверов Windows NT 4.0 класса BDC.

Для надлежащей работы BDC-контроллера Windows NT 4,0 ему требуется получать обновления информации с серверов PDC. Поэтому один контроллер домена Windows Server 2003 играет роль BDC-контроллера Windows NT 4.0, что позволяет тиражировать изменения на любой из серверов BDC Windows NT 4.0 в этом домене. Выполняя подобную функцию, контроллер домена Windows Server 2003 играет *роль единого гибкого хозяина операций (Flexible Single Master Operations* (FSMO) *role*), также известную как роль ведущего узла. Эта специальная роль сервера называется *эмулятором PDC*.

Даже в развитой среде, основанной исключительно на использовании Windows Server 2003, *хозяин операций* — эмулятор PDC — по-прежнему играет важную роль в создании системы. Он выполняет определенные обязанности, с которыми не может справиться никакой другой контроллер домена. Эмулятор PDC обладает преимуществом в получении копий изменений паролей, выполняемых другими контроллерами домена. При изменении пароля для распространения изменений на каждый контроллер домена требуется время. Эта задержка на синхронизацию может вызвать ошибку идентификации в контроллере домена, который еще не получил изменений. Прежде чем этот контроллер удаленного домена запретит доступ всему, что стремится этот доступ получить, он перенаправит запрос на идентификацию эмулятору PDC, поскольку эмулятор PDC может владеть другой информацией (например, новым паролем).

При работе домена в смешанном режиме клиенты могут использовать имена NetBIOS для доступа к устаревшим службам домена либо могут использовать Active Directory для доступа к службам домена Windows Server 2003. Чтобы обнаружить контроллер домена Windows Server 2003, клиент должен послать запрос DNS-серверу для получения служебной записи, которая принимает общую форму:

```
_ldap._tcp.<имя домена>.
```

где `_ldap._tcp.dummies.com` представляет, к примеру, контроллеры домена для домена `dummies.com`.

Контроллеры домена Windows Server 2003 не обязаны запускать службу DNS локально. Единственное требование заключается в том, чтобы DNS-серверы поддерживали требуемые типы служебных записей, что позволяет обнаружить контроллеры этого домена.

Что заставляет работать Active Directory

Active Directory реализована с использованием структуры каталога данных на основе стандарта X.500, интерфейса LDAP для доступа к данным каталога и динамической службы DNS в качестве механизма локализации данных каталога. Теперь, когда вы знаете все эти подробности, касающиеся Active Directory, что это дает вам? В приведенном ниже списке перечислены некоторые основные особенности и преимущества Active Directory.

- ✓ Безопасность. Информация хранится в защищенном виде. Каждый объект Active Directory снабжен *списком управления доступом (Access Control List — ACL)*, содержащим перечень ресурсов, которые могут получить к нему доступ, а также перечень полномочий доступа, предоставленных каждому такому ресурсу.
- ✓ Возможности формирования запросов. Active Directory генерирует *глобальный каталог (global directory)*, способный обеспечить гибкий механизм обработки запросов. Любой клиент, поддерживающий Active Directory, может послать запрос на получение данных каталога.
- ✓ **Тиражирование.** Тиражирование каталога на все контроллеры доменов в домене означает более легкий доступ, более высокую готовность и лучшую отказоустойчивость.
- ✓ Расширяемость. Служба Active Directory — *расширяема*, а это означает, что в каталог можно добавить новые типы объектов либо *расширить* существующие объекты.

Например, вы можете легко добавить к объекту типа "работник" атрибут типа "зарплата" или добавить идентификатор работника к пользовательскому объекту, (Атрибут — это дополнительная информация об объекте.)

- ✓ Поддержка нескольких протоколов. При взаимодействии серверов каталогов либо в рамках каталогов от разных поставщиков могут использоваться различные сетевые протоколы, поскольку в основе Active Directory лежит стандарт X.500. В настоящее время к этим протоколам относятся LDAP версий 2 и 3 и *HTTP (Hypertext Transfer Protocol — протокол передачи гипертекстовых файлов)*. Естественно, сторонние поставщики по мере необходимости могут расширять возможности по включению и других протоколов.
- ✓ Распределение информации. В среде Active Directory информация может быть распределена по доменам, чтобы избежать необходимости тиражировать большие объемы данных каталога. Каждый такой домен называется *деревом (tree),* поскольку его каталог в соответствии со стандартом X.500 представляет собой дерево с единственным корнем. В больших и сложных сетях совокупность доменов образует группу деревьев, которая (вы угадали) называется *лесом*!

Разделение данных Active Directory на несколько различных деревьев не означает, что информацию от Active Directory нельзя запросить из других доменов. *Глобальный каталог* содержит подмножество информации о каждом объекте во всем лесе домена. Это позволяет осуществлять поиск информации по всему лесу домена посредством содействия ваших дружественных локальных контроллеров доменов.

Что означает тиражирование

В домене Windows Server 2003 все контроллеры доменов равны. Поэтому при применении изменений к любому из контроллеров домена каталоги домена всех других контроллеров домена должны быть полностью обновлены за счет записи этих изменений (с помощью упомянутого в предыдущем разделе процесса *тиражирования с несколькими ведущими узлами*).

Вот как осуществляется тиражирование с несколькими ведущими узлами: чтобы следить за изменениями и обновлением объектов Active Directory, эта служба использует специальный номер — USN (Update Sequence Number — порядковый номер обновления). По мере того как объект изменяется, этот номер увеличивается на единицу для каждого объекта, который подвергся изменениям. Например, объект учетной записи пользователя, который был изменен для включения в него информации о телефонном номере, должен на единицу увеличить свой UNS-номер, чтобы отразить произведенную модификацию. Затем это модифицированное значение объекта отправляется другим контроллерам домена. Объект с самым большим значением UNS-номера, т.е. обновленный объект, перезаписывается поверх объекта с меньшим UNS-номером.

Наращивание UNS-номера — *атомическая операция (atomic operation)*; на обычном языке это означает, что увеличение значения UNS-номера и фактическое изменение данных каталога происходят одновременно. Если одна из частей операции оканчивается неудачей, то считается, что все изменение окончилось неудачно; поэтому невозможно изменить какой-либо объект Active Directory без увеличения его UNS-номера. Таким образом, ни одно из изменений не может быть утеряно. Каждый из контроллеров домена следит за самыми большими UNS-номерами других контроллеров домена, с которыми он обменивается копиями записей об изменении. Это позволяет контроллеру домена вычислять, какие изменения должны быть тиражированы в каждом цикле тиражирования. Попросту говоря, самый большой UNS-номер всегда выигрывает!

Деревья доменов

Дерево доменов — это набор доменов Windows Server 2003 или доменов Windows 2000 (или тех и других), связанный двусторонним транзитивным доверительным отношением и разделяющий общую схему, конфигурацию и глобальный каталог. Набор доменов можно рассматривать в качестве дерева доменов только в том случае, если входящие в него домены образуют непрерывное иерархическое пространство имен. Отдельный домен сам по себе без дочерних имен также рассматривается как дерево.

Первый домен, установленный в дереве доменов, представляет собой *корневой домен* (*root domain*) этого дерева. Он рассматривается как *корневой домен леса* (*forest root domain*), если он также является первым доменом леса. Лес *Active Directory* состоит из одного или нескольких доменов Windows 2000 или доменов Windows Server 2003 (или тех и других), которые совместно используют общую схему, конфигурацию и глобальный каталог. Пространство имен леса Active Directory не является непрерывным.

Все домены дерева доменов и все деревья в отдельном лесу пользуются преимуществом взаимодействия на основе двустороннего транзитивного доверительного отношения, которое устанавливается как доверительное отношение по умолчанию между доменами Windows 2000 и Windows Server 2003. Это полное доверие между всеми доменами, входящими в иерархию доменов Active Directory, способствует формированию леса как единого образования за счет его общей схемы, конфигурации и глобального каталога.

В начале каждого цикла тиражирования каждый контроллер домена проверяет свою таблицу UNS-номеров и посылает запрос о последних UNS-номерах всем другим контроллерам домена, которые входят в схему тиражирования. Рассмотрим в качестве примера следующую таблицу, которая содержит UNS-номера для сервера A.

Контроллеры домена	UNS-номер
Контроллер домена B	54
Контроллер домена C	23
Контроллер домена D	53

Затем сервер A запрашивает у контроллеров домена их текущие UNS-номера и получает такие результаты.

Контроллеры домена	UNS-номер
Контроллер домена B	5B
Контроллер домена C	23
Контроллер домена D	64

Используя эти данные, сервер A может вычислить номера изменений, которые ему необходимо получить от каждого сервера.

Контроллеры домена	UNS-номер
Контроллер домена Б	55, 56, 57, 58
Контроллер домена C	Новейшая информация
Контроллер домена D	54-64

После этого он может запросить у каждого из серверов необходимую информацию об изменениях.

Векторы последних изменений (Up-to-Date Vector) представляют собой два различных сегмента данных, которые содержат *уникальный глобальный идентификатор (Globally Unique Identifier — GUID)* и уже рассмотренный нами порядковый номер обновления — USN. Вектор последних изменений состоит из пар UNS-номеров серверов, принадлежаших двум контроллерам домена, которые содержат самые большие номера для инициированных ими обновлений. (Обычно это контроллер домена, который является источником обновления, и его ближайший партнер по схеме тиражирования.) Вектор наивысшей отметки (High Watermark Vector) содержит самое большое значение атрибута USN для любого заданного объекта. Используя оба этих вектора, контроллер домена может определить, что данная копия данных уже была получена, чтобы предотвратить дальнейшее тиражирование этого конкретного обновления.

Поскольку объекты обладают свойствами, они также обладают и *номером версии свойства (Property Version Number — PVN)*. Каждое свойство объекта обладает PVN-номером, и всякий раз при модификации этого свойства его PNV увеличивается на единицу. (Звучит знакомо?) Эти номера PNV используются для определения конфликтов, которые происходят при внесении нескольких изменений в некоторое свойство объекта. При наступлении конфликта преимущество получает изменение с самым большим значением PNV-номера.

Если и PNV совпадают, для разрешения подобного конфликта используется временная метка *(time stamp)*. Временные метки — отличная вторая линия защиты, позволяющая избежать конфликтов. Они в явном виде указывают на время внесения изменений в данные каталога, позволяя, таким образом, системе определить, должно ли одно изменение в действительности иметь преимущество перед другим.

В случае чрезвычайно маловероятного события совпадения номеров PNV *и* временных меток проводится сравнение двоичных буферов и преимущество отдается буферу большего объема. Номера PNV (в отличие от UNS) увеличиваются только при записи первоначального изменения, а не при записи копии изменения. PNV-номера не являются специфической принадлежностью сервера, а "путешествуют" вместе со свойствами объекта.

Чтобы остановить информацию об изменениях, которая повторно посылается другим серверам, используется затухание распространения изменений. Схема затухания распространения изменений используется сервером Windows Server 2003, чтобы предотвратить бесконечные логические циклы тиражирования обновлений в структуре Active Directory и воспрепятствовать избыточной передаче изменений к серверам с уже обновленным состоянием.

О главной схеме

Каждый объект леса Active Directory составляет часть одной и той же схемы. Схема определяет различные типы информации, которую могут хранить объекты активного каталога в Active Directory. Схема включает два основных определения данных: атрибуты и классы.

Например, объект-пользователь обладает такими атрибутами, как имя, адрес и телефонный номер. Совокупность этих атрибутов и их определений называется схемой. Вы можете представить себе схему объекта как длинный список его атрибутов или контрольный перечень его возможностей, Схема, применяемая по умолчанию, обеспечивает определения для пользователей, компьютеров, доменов и т.п. На каждый объект в домене приходится только одна схема, поскольку один и тот же объект не может обладать несколькими определениями.

Определение схемы, используемой по умолчанию, задается в файле SCHEMA.INI, который также содержит начальную структуру для файла NTDS.DIT, хранящего данные Active Directory. Файл SCHEMA.INI расположен в каталоге `%systemroot%\ntds`, это ASCII-файл, и его содержимое можно просмотреть на экране или распечатать.

К редактированию схемы Active Directory нельзя относиться с легкостью. Например, вы легко можете добавить атрибут "зарплата" или идентификатор работника к объекту-пользо-

вателю. В большинстве случаев вы должны поручать редактирование схемы наиболее опытным программистам или системным администраторам, поскольку изменения, вносимые в схему, нельзя отменить и неверное редактирование может серьезно повредить Active Directory и сказаться на всем лесе доменов. Если на вашей машине установлены некоторые приложения, например Exchange Server, они могут брать редактирование схемы на себя. Если по какой-либо причине вы имеете желание отредактировать схему, прилягте и подождите, пока это желание пройдет. Если оно вас не покидает, обратитесь к профессионалу по программированию Active Directory.

Лес доменов всего предприятия (совокупность деревьев Active Directory в одном контейнере-организации) использует одну общую схему. Если вы изменяете эту схему, это влияет на каждый из контроллеров доменов в каждом подключенном домене. Поэтому вы должны быть твердо уверены в том, что любые вносимые вами изменения и корректны, и допустимы. Изменения в схему должны вносить только опытные программисты или администраторы схемы. Более подробную информацию о расширении схемы можно найти в "Руководстве программиста по Active Directory" (Active Directory Programmer's Guide) на Web-узле Microsoft (www.microsoft.com).

Глобальный каталог

Глобальный каталог содержит входы для всех объектов одного леса Active Directory (т.е. совокупности деревьев доменов, которые могут совместно использовать или не использовать единое непрерывное пространство имен). Он содержит все свойства для всех объектов его собственного домена, а также содержит частичное подмножество свойств всех остальных объектов леса. Лес в целом использует общий глобальный каталог. Несколько серверов содержит копии всего каталога; эти серверы представляют собой контроллеры доменов, называемые *серверами глобального каталога*. Чтобы поддерживать копию глобального каталога, сервер должен поддерживать копию Active Directory, что автоматически делает сервер контроллеромдомена.

Операции поиска в пределах всего леса ограничены рамками свойств объектов, которые принадлежат глобальному каталогу. Чтобы отыскать любое свойство в пределах локального пользовательского домена, вы можете воспользоваться так называемым *глубоким поиском* вне пределов глобального каталога.

Не стоит включать в конфигурацию слишком много глобальных каталогов для каждого домена, поскольку тиражирование, необходимое для поддержки таких каталогов, может оказаться непосильной ношей для сети. Обычно достаточно одного глобального сервера каталога на узел.

Хотя область поиска может включать любой заданный контейнер или организационную единицу в пределах определенного домена, определенного дерева доменов или леса в целом, в большинстве случаев полный поиск связан с формированием запросов ко всему лесу Active Directory через глобальный каталог.

Планирование развертывания Active fiirecton/

Если вы используете определенную версию Windows NT, в вашем распоряжении может быть несколько доменов с определенными доверительными отношениями между отдельными парами доменов. Теоретически вы можете просто обновить каждый домен, сохранив при

этом существующие доверительные отношения и не внося никаких изменений. Однако в результате такого подхода вы утратите преимущества, свойственные Active Directory.

Если вы эксплуатируете домен Windows 2000, все равно кое-что необходимо спланировать. Хотя серверы Windows Server 2003 и Windows 2000 могут выступать в качестве контроллеров одного и того же домена, мы, в общем случае, не рекомендуем вам использовать две версии продукта для выполнения одной функции. В большинстве случаев применение в точности одной и той же версии операционной системы (включая обновления и "заплаты") позволит избежать неожиданных неполадок, приводящих к разрушению вашего домена и выходу из строя всей сети.

Учитывая сказанное, вы можете развернуть системы Windows Server 2003 в доменах в качестве контроллеров домена. Вы можете даже модернизировать Windows 2000 до Windows Server 2003, чтобы превратить контроллер домена Windows 2000 в контроллер домена Windows Server 2003. Просто будьте осторожны. Не модифицируйте одновременно все системы. Модифицируйте одну или две системы, а затем проведите всесторонние испытания, чтобы убедиться, что система по-прежнему выполняет все ожидаемые функции. Всегда оставляйте себе путь к отступлению — возможность сделать откат к предыдущей конфигурации, где все работало нормально.

В большинстве случаев организации, уже использующие Windows 2000, не станут без промедления переходить на Windows Server 2003. Наиболее вероятные кандидаты для перехода на Windows Server 2003 — предприятия, использующие Windows NT, которые ожидают второго поколения серверов Active Directory от Microsoft, прежде чем последовать массовому примеру. Поэтому остаток дискуссии, посвященной переходу на Windows Server 2003, концентрируется на модификации Windows NT. Если вам требуется переход с Windows 2000, кое-что из последующих рассуждений может пригодиться, но оно почти очевидно.

Прежде чем модифицировать один из контроллеров доменов, вам необходимо разработать план развития вашего домена. Затем вы должны использовать этот план для управления порядком и методом перехода с доменов Windows NT к Active Directory для Windows Server 2003.

Пространство имен

Пространство имен (namespace) — это логически связанная область, которая содержит имена, основанные на стандартизированном соглашении о символическом представлении объектов или информации. Создание имен внутри пространства имен и способ применения имен к объектам подчиняются определенным правилам. Многие пространства имен по своей природе отличаются иерархической структурой, подобной пространствам имен, используемым службами DNS и Active Directory. Другие пространства имен, например имена NetBIOS, неструктурированы и отличаются линейным характером.

В системе Windows Server 2003 домены используют более развитую систему DNS-имен в сравнении с именами NetBIOS. За счет этого между доменами устанавливаются отношения типа "родитель-потомок" (когда один домен может быть создан как "дочерний" по отношению к другому), чего не может поддерживать Windows NT. Например, `sales.dummies.com` — дочернин домен домена dummies . com. (Дочерний домен всегда содержит полное имя родительского домена внутри своего **собственного** имени.)

Важно помнить, что отношения типа "родитель-потомок" можно создать только внутри родительского домена с использованием мастера установки Active Directory — утилиты DCPROMO. Родительский домен должен существовать до того, как вы создадите для него дочерний домен. Поэтому порядок, в котором вы создаете или модифицируете ваши домены, имеет решающее значение!

В следующем разделе приводятся дополнительные, важные причины создания доменов в определенном порядке. Но прежде чем вы озаботитесь вопросами узлов, вам необходимо знать, что корневой домен предприятия всегда должен создаваться до того, как вы приступите к созданию любых других доменов. Например, если вы начали с создания корневого домена dummies.com домен sales.dummies.com и все другие зависимые домены могут быть созданы как дочерние домены корневого домена dummies.com. Подобная структура помогает при операциях поиска в других доменах и открывает возможность перевода доменов под управление будущих версий Windows Server 2003.

Создание узлов

Узлы в Active Directory используются для группирования серверов в рамках контейнеров, которые зеркально отображают физическую схему вашей сети. Подобная организация позволяет вам настроить конфигурацию процесса тиражирования между контроллерами доменов. В действительности узлы в первую очередь используются для управления тиражированием через более медленные каналы глобальной сети между отдельными сегментами одной и той же сети. Некоторое количество подсетей TCP/IP также можно отобразить на узлы, что позволяет новым серверам присоединяться к надлежащему узлу автоматически, в зависимости от их IP-адресов. Подобная схема адресации также облегчает для клиентов поиск ближайшего к ним контроллера домена.

При создании первого контроллера домена по умолчанию создается узел Default-First-Site и контроллер домена приписывается этому узлу. Последующие контроллеры доменов добавляются к этому узлу, но их можно переместить. Вы можете также переименовать этот узел так, как считаете нужным.

Администрировать и создавать узлы можно с помощью утилиты Active Directory Site and Services, интегрированной с Microsoft Management Console (MMC). Чтобы создать новый узел, выполните следующие действия.

1. **Запустите утилиту Active Directory Site and Services (Start⇨Administrative Tools⇨Active Directory Site and Services) (Пуск⇨Администрирование⇨Active Directory — сайты и службы).**
2. **Щелкните правой кнопкой мыши на ветви Sites (Узлы) и выберите компонент New Site (Новый** узел).

   Появится диалоговое окно New Object — Site (Новый объект — Сайт).
3. **Ведите имя для узла (например, New York).**

   Имя должно состоять не более чем из 63 символов и не содержать символов точки ('.') и пробела. Вы также должны выбрать связь узла из списка. По умолчанию при выполнении процесса DCPROMO создается связь DEFAULTIPSITELINK. Если вы не создаете дополнительные узлы вручную, это будет единственная связь в списке.
4. **Выберите связь узла, чтобы привязать новый узел, а затем щелкните на кнопке OK.**
5. **Прочтите сообщение в диалоговом окне, подтверждающее создание узла, а затем щелкните на кнопке OK.**

Теперь, после того как узел создан, вы можете назначить ему различные IP-подсети. Для этого выполните следующие действия.

1. **Запустите утилиту Active Directory Site and Services (Start⇨Administrative Tools⇨Active Directory Site and Services) (Пуск⇨Администрирование⇨Active Directory — сайты и службы).**

2. **Раскройте ветвь Sites.**
3. **Щелкните правой кнопкой мыши на компоненте Subnets (Подсети) и выберите опцию New Subnet (Новая подсеть).**

   Появится диалоговое окно New Object — Subnet (Новый объект — Подсеть).
4. **Введите имя подсети в виде <сеть>/<замаскированные биты>.**

   Например, 200.200.201.0/24 представляет сеть 200.200.201.0 с маской подсети 255.255.255.0
5. **Выберите узел, с которым ассоциирована подсеть, например New York.**
6. **Щелкните на кнопке OK.**

Теперь в вашем распоряжении имеется подсеть, связанная с узлом. При желании вы можете назначить узлу несколько подсетей. Подсети рассматриваются в главе 14. Еще более подробную информацию можно получить в разделе подсетей меню Help Windows Server 2003.

Организационные единицы

Производственное подразделение (*organizational unit —OU*) — ключевой компонент протокола X.500. Как следует из названия, организационная единица содержит объекты домена. Организованные в виде логического контейнера, что обеспечивает более тонкое разделение и управление в рамках домена, контейнеры организационных единиц могут содержать другие организационные единицы, группы, пользователей и компьютеры.

Организационные единицы могут быть вложены друг в друга, образуя иерархию, которая совпадает со структурой вашего предприятия или организации. Используя организационные единицы, вы можете исключить необходимость в громоздких моделях, разрабатываемых для доменов на основе Windows NT Server (например, модели главного домена, в которой несколько доменов-ресурсов используют учетные записи одного центрального домена-пользователя). С помощью Active Directory вы можете создать один большой домен и группу ресурсов и пользователей в нескольких отдельных организационных единицах.

Самое существенное преимущество организационных единиц заключается в том, что они позволяют вам делегировать полномочия. Вы можете назначить определенным пользователям или группам права административного контроля организационной единицы, которые позволяют им изменять пароли и создавать учетные записи в этой организационной единице, но не предоставлять им права на управление остальной частью домена. Эта возможность представляет собой основное усовершенствование по сравнению с администрированием доменов в Windows NT, где использовался принцип "все или ничего".

Установка Active Directory

При работе с Windows NT вы задаете тип каждого из серверов в процессе установки. Функции сервера могут соответствовать одной из следующих ролей.

- ✓ Отдельный/рядовой сервер.
- ✓ PDC-контроллер.
- ✓ BDC-контроллер.

За исключением смены ролей PDC-контроллер/BDC-контроллер другие роли сервера нельзя изменить без переустановки ПО. Например, невозможно изменить рядовой сервер на контроллер домена без переустановки Windows NT.

С появлением сервера Windows Server 2003 все эти проблемы остались позади, и вы имеете возможность установить все серверы как обычные. Вы можете воспользоваться мастер-программой (рассматриваемой в следующем разделе), чтобы преобразовать обычный сервер в контроллер домена или, наоборот, контроллер домена — в обычный сервер. Эта функциональность также дает вам возможность перемещать контроллеры доменов из одного домена в другой с помощью понижения ранга контроллера домена до рядового сервера с последующим повышением его ранга до контроллера домена в другом домене. В среде Windows NT понижение и повышение ранга контроллеров доменов обычно требует переустановки операционной системы или специальных ухищрений.

Изменение ранга серверов

Windows Server 2003 позволяет вам превратить сервер из обычного сервера в контроллер домена и наоборот. Для этого используется утилита Active Directory Installation Wizard. Доступ к этой утилите можно получить посредством программы настройки конфигурации Configure Your Server (Start⇨All Programs⇨Administrative Tools⇨Configure Your Server — см. главу 10) или с помощью утилиты DCPROMO, которая запускается командой Run (Выполнить) или из командной строки. Мастер-программу Active Directory Installation Wizard можно использовать также для удаления Active Directory из контроллера домена; при этом система возвращается к состоянию рядового сервера. Пошаговая процедура установки Active Directory и создания контроллера домена описана в главе 10.

База данных Active Directory и общий системный том

Хотя вы должны представлять себе Active Directory этаким информационным "фонтаном", эта информация хранится в виде файла на каждом контроллере домена в файле `%systemroot%\NTDS\ntds.dit`. Этот файл всегда открыт, и из него нельзя сделать резервную копию с помощью простой операции копирования. Однако, аналогично старому методу резервного копирования SAM в Windows NT, новая программа NTBACKUP, входящая в состав Windows Server 2003, включает возможность получения и мгновенного снимка Active Directory, и резервной копии этой информации (эта функция называется System State — состояние системы). Существует даже специальный *режим восстановления каталога (directory restoration mode),* в котором следует загрузить систему, чтобы восстановить резервную копию Active Directory! (Подробно резервное копирование будет рассмотрено в главе 17.)

Общий системный том (share system volume), или SYSVOL, — корневой каталог тиражирования для каждого домена. Его содержимое тиражируется на каждый из контроллеров домена, использующего службу тиражирования файлов (File Replication Service). Том SYSVOL должен располагаться на томе с файловой организацией NTFS 5.0, поскольку это требование службы тиражирования файлов.

Том SYSVOL представляет собой также совместно используемый том, указывающий (по умолчанию) на каталог `%systemroot%\SYSVOL\sysvol`, который содержит специфические для домена области наподобие сценариев входа в систему. Например, разделяемый файл регистрации NETLOGON для домена savilltech.com указывает на сценарии `%systemroot%\SYSVOL\sysvol\savilltech.com\SCRIPTS`. Вы можете просто скопировать файлы, используемые для входа и выхода из домена, в этот каталог, и изменения будут скопированы во все другие контроллеры доменов в следующем цикле тиражирования (который по умолчанию устанавливается равным 15 минутам).

Режимы работы домена

Домены Windows Server 2003 работают в четырех режимах: смешанном, собственном, .NET и промежуточном .NET. *Домены в смешанном режиме (mixed-mode domain)* позволяют BCD-контроллерам Windows NT 4.0 участвовать в работе доменов Windows Server 2003. В *собственном режиме (native mode)* в работе домена могут принимать участие только контроллеры доменов на основе Windows Server 2003 и Windows 2000, а BCD-контроллеры на основе Windows NT 4.0 не могут больше работать как контроллеры доменов. В *режиме .NET (.NET mode)* в качестве контроллеров доменов могут работать только серверы, работающие под управлением Windows Server 2003. *Промежуточный режим .NET (.NET interim mode)* используется при наращивании домена Windows NT 4.0 до первого домена в новом лесу Windows 2003.

Переключение из смешанного режима в собственный или из собственного в .NET-режим — необратимая операция, поэтому не изменяйте режим до тех пор, пока все контроллеры домена не будут переведены под управление Windows Server 2003 или Windows 2000 для собственного режима или под управление Windows Server 2003 для режима .NET. Кроме того, после переключения режима вы не сможете добавить к домену ни один BCD-контроллер на основе Windows NT 4.0.

Переключение в собственный режим позволяет использовать *универсальные группы (universal group)*, которые, в отличие от глобальных групп, могут быть вложены одна в другую. Старые клиенты на основе NetBIOS по-прежнему имеют возможность входить в систему, используя NetBIOS-имя домена даже в собственном режиме, Универсальные группы также поддерживаются в режиме .NET.

Изменение режима домена известно как повышение функциональности домена. Вы можете выбрать вариант перехода в собственный режим из смешанного режима, перехода в режим .NET из собственного режима или совершить скачок прямо в режим .NET из смешанного режима. Но будьте осторожны: это дорога в один конец. Чтобы вернуться к более низкому уровню функциональности, после того, как вы его повысили, вам придется переустановить систему.

Чтобы повысить уровень функциональности, выполните следующие действия на контроллере домена Windows Server 2003.

1. **Запустите утилиту Active Directory Domains and Trusts (Start⇨Administrative Tools⇨Active Directory Domains and Trusts) (Пуск⇨Администрирование⇨ Active Directory — Домены и доверие).**
2. **Выберите домен, который вы намерены изменить.**
3. **Выберите команду Action⇨Raise Domain Functional Level (Повысить уровень функциональности домена).**

   Появится диалоговое окно Raise Domain Functionality (Повысить функциональность домена).

4. **Воспользуйтесь выпадающим списком для выбора режима Windows 2000 native mode или Windows .NET Server mode, а затем щелкните на кнопке Raise (Повысить).**

   На экране отобразится сообщение, подтверждающее выполнение операции.

5. **Щелкните на кнопке OK.**

   На экране отобразится предупреждение о том, что изменение режима домена вступит в силу через 15 минут.

6. **Щелкните на кнопке OK.**

Вам также необходимо проверить все остальные контроллеры доменов в домене. Убедитесь в том, что для каждого домена в диалоговом окне свойств отображается корректное значение для режима (щелкните правой кнопкой мыши на имени домена и выберите опцию Properties). Если ни для одного из контроллеров доменов изменения не отображаются через 15–20 минут, перезагрузите сервер. Это инициирует процесс тиражирования.

Если при внесении изменений вам не удается установить контакт с контроллером домена (например, он расположен на удаленном узле и соединяется с главным узлом только периодически), удаленный контроллер домена переключит свой режим при выполнении очередной процедуры тиражирования,

Когда домены множатся

В этом разделе вы ознакомитесь с новыми методами соединения доменов, доступными в Windows Server 2003. При работе с доменами Windows NT 4.0 вы были ограничены простыми одно- или двухнаправленными доверительными отношениями для явного соединения двух доменов одновременно. Система Windows Server 2003 обладает намного более развитыми функциональными моделями для создания отношений и соединений доменов, созданных на ее основе.

Доверительные отношения между доменами

Доверительные отношения в системе Windows NT 4.0 не обладают свойством транзитивности. Например, если домен А "доверяет" домену В, а домен С "доверяет" домену В, домен С не "доверяет" автоматически домену А (рис. 11.2).

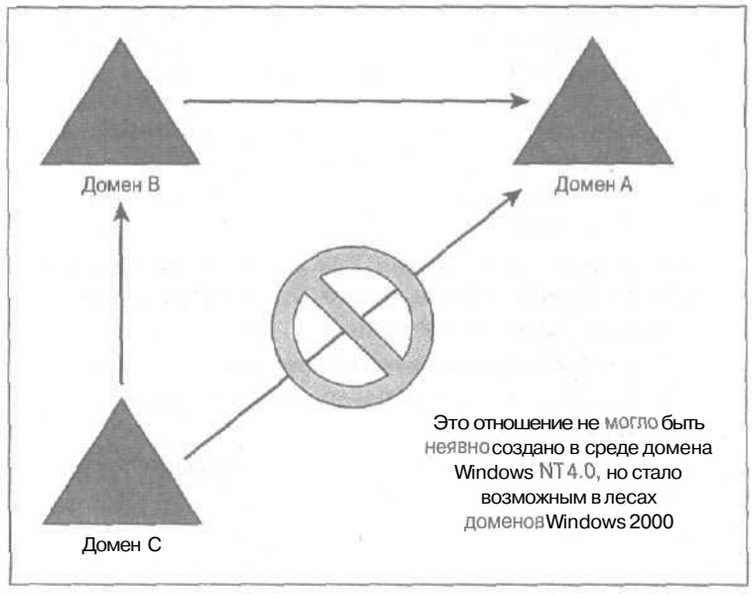


***Рис.** 11.2. **Пример** доверительного отношения в Windows NT 4.0*

Подобное отсутствие транзитивности больше не имеет места для доверительных отношений, используемых для соединения доменов, — компонентов дерева или леса в системах Windows Server 2003 и Windows 2000. Доверительные отношения, используемые в деревьях Windows Server 2003 и Windows 2000, представляют собой двусторонние транзитивные доверенности. Это означает, что любой домен леса неявно "доверяет" каждому другому домену в

его дереве или лесе. Это избавляет от необходимости выполнения трудоемкого администрирования отдельных доверенностей между парами доменов, поскольку подобные доверенности создаются автоматически, как только новый домен присоединяется к дереву.

Безопасность доверительных отношений в системе Windows Server 2003 поддерживается за счет применения системы Kerberos. Протокол *Kerberos Version 5.0* представляет собой основной протокол системы защиты для Windows Server 2003, однако этот протокол разработан не Microsoft. Система Kerberos — система защиты, разработанная в Массачусетсском технологическом институте. Она проверяет как подлинность пользователя, так и целостность всех сеансовых данных после регистрации этого пользователя. Служба Kerberos устанавливается на каждом контроллере домена, а клиент Kerberos устанавливается на каждой рабочей станции и сервере. Начальная идентификация пользователя в системе Kerberos гарантирует, что доступ к корпоративным ресурсам пользователь получает с помощью одного и того же пароля для входа в систему. Более подробную информацию о системе Kerberos можно найти в документах Requests for Comments 1510 и 1964, разработанных IETF (Internet Engineering Task Force — Проблемная группа проектирования Internet). Эти документы доступны на Web-узле `www.rfc-editor.org`.

Создание деревьев

В Windows Server 2003 один домен может быть "потомком" другого домена. Например, домен `legal.savilltech.com` является "потомком" домена `savilltech.com` (который является именем корневого домена и, таким образом, именем дерева). Дочерний домен всегда содержит полное имя родительского домена. Как показано на рис. 11.3, домен `dev.savillCORP.com` не может быть "потомком" `savilltech.com`, поскольку имена доменов не сопоставимы. Дочерний домен и его "родитель" совместно используют двустороннюю транзитивную доверенность.

Когда один домен является "потомком" другого, возникает *лес доменов*. Лес доменов должен обладать непрерывным пространством имен (это означает, что все пространство имен использует общий корень, т.е. имеет одного и того же "родителя").

Деревья доменов можно создавать только в процессе преобразования "сервер-контроллер домена" с помощью утилиты DCPROMO.EXE.

Помещение домена в дерево обладает рядом преимуществ. Первое и самое значительное преимущество состоит в том, что все компоненты дерева обладают транзитивными доверительными отношениями со своим "родителем" и со всеми своими "потомками", управляемыми системой. Эти транзитивные доверительные отношения также означают, что любому пользователю или группе в дереве домена может быть предоставлен доступ к любому объекту в пределах всего дерева. Кроме того, на любой рабочей станции дерева доменов можно использовать единый пароль для входа в систему.

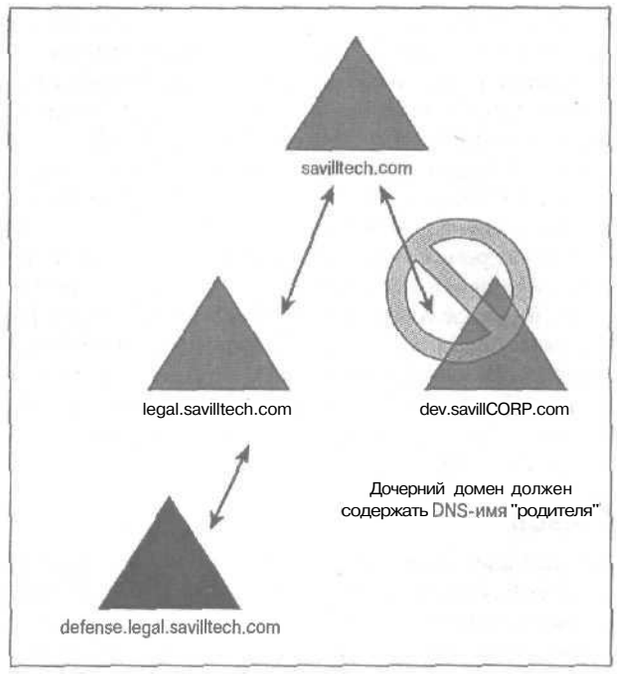


Рис. 11.3. Примеротношения "родитель–потомок"

Что такое лес

В вашей организации может быть несколько отдельных деревьев доменов, которые совместно используют общие ресурсы. Вы можете передать ресурсы в совместное использование нескольким деревьям за счет объединения этих деревьев в виде леса.

Лес — это совокупность деревьев, которые в явном виде не используют совместно единое непрерывное пространство имен (однако пространство имен каждого дерева по-прежнему должно оставаться непрерывным).

Например, как показано на рис. 11.4, два корневых домена объединены с помощью двусторонней Kerberos-доверенности (наподобие доверенности, создаваемой между "потомком" и его "родителем"). Лес всегда содержит все дерево доменов каждого домена, и вы не можете создать лес, который содержит только часть дерева доменов.

Леса создаются при инициировании первого процесса преобразования "сервер–контроллер домена" с помощью утилиты DCPROMO.EXE, и их нельзя создать в какой-либо другой момент.

Вы не ограничены только двумя деревьями доменов в лесу. (Вы можете иметь в своем распоряжении лес только из одного дерева, поскольку сам по себе отдельный домен технически рассматривается и как дерево, и как лес.) Вы можете добавить столько деревьев, сколько вам необходимо, и все деревья, включенные в лес, обладают возможностью получить права доступа к объектам для любого пользователя, входящего в лес. (Что, конечно же, уменьшает необходимость управления доверительными отношениями вручную.) Ниже перечислены основные преимущества лесов.

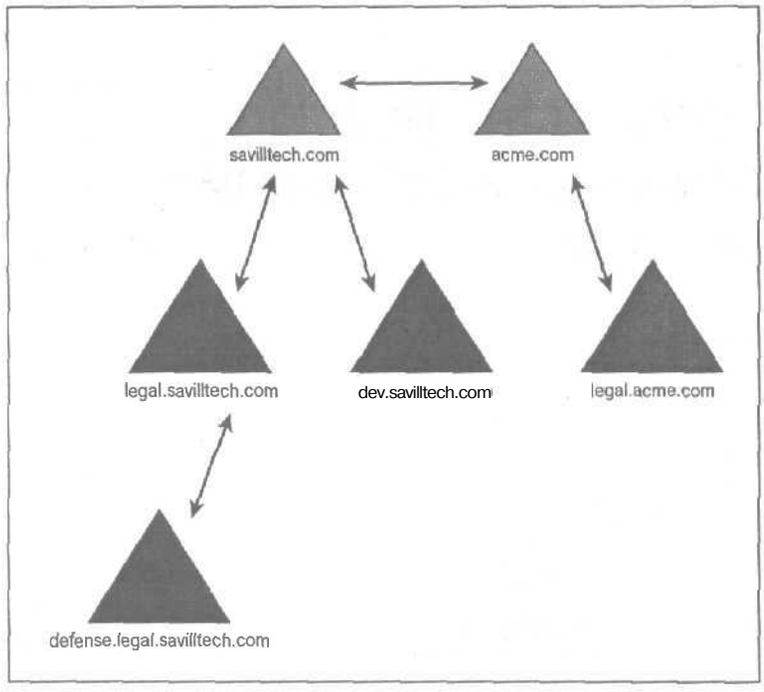


Рис. 11.4. Пример леса

- ✓ Все деревья обладают общим глобальным каталогом, содержащим специфическую информацию о каждом объекте леса.
- ✓ Все деревья содержат общую схему. До сих пор Microsoft не объяснила, что произойдет, если два дерева обладают различными схемами перед их объединением. Мы предполагаем, что изменения будут подвергнуты слиянию.
- ✓ Поиск в лесу приводит к глубокому поиску в рамках всего дерева домена, который является инициатором запроса, при этом для остальной части леса используются входы глобального каталога.

Глава 12

Работаем с Active Directory, доменами и доверительными отношениями

В этой главе...

- Осваиваем домены
- Управление доменами и каталогами
- Обработка разрешений для каталогов
- Управление доверенностями

Все великолепные возможности Active Directory будут бесполезны, пока вы не сможете настраивать ее содержимое и манипулировать им. Только тогда вы сможете в полной мере воспользоваться ее мощной (но таинственной) средой. В этой главе мы пристально приглядимся к Active Directory. Однако, прежде чем вы увидите ее содержимое во всем блеске на ваших экранах, мы намерены показать вам, как манипулировать и настраивать конфигурацию содержимого в тесной связи с манипулированием и настройкой конфигурации доменов. Да, это так; вам придется приняться за домены еще раз. Итак, дорогие друзья, пусть ваши героические усилия не пропадут даром, и вы наверняка станете хозяином своего домена.

Подробная информация о контроллерах доменов и изменении их роли в Windows 2003 представлена в главе 11.

Хозяин вашего домена

Роли контроллера домена определяются не в процессе установки Windows Server 2003, а с помощью утилиты Active Directory Installation Wizard. (Более подробно о мастер-программе Active Directory Installation Wizard рассказывалось в главе 11.) Система Windows Server 2003 заимствовала концепцию основного контроллера домена (PDC) из Windows NT посредством использования эмулятора PDC для выполнения определенных функций контроллера, но она отказалась от концепции резервного контроллера домена (BDC). В Windows 2003 все контроллеры доменов равны и связаны равноправными отношениями, а не играют роль главного (PDC) и подчиненного (BDC) в отношении "главный-подчиненный".

Чтобы поддерживать устаревшие BDC-контроллеры Windows NT 4.0 и Windows NT 3.51 в среде со смешанным режимом (mixed-mode), один из контроллеров доменов Windows Server 2003 должен эмулировать работу PDC-контроллера Windows NT Server 4.0. В таком случае он должен тиражировать изменения на эти устаревшие BDC-контроллеры, чтобы они могли осуществить необходимые изменения, например модификацию паролей.

Если не проявлять осторожность, все эти равноправные контроллеры могут вызвать проблемы. (Знаете поговорку "У семи нянек дитя без глазу"?) Чтобы поддерживать порядок среди всех этих равноправных узлов, в Windows Server 2003 предусмотрены пять специальных ролей. Одна из ролей специально была рассчитана на поддержку "старомодных" клиентов Windows NT и контроллеров доменов. Остальные четыре роли предназначены для того, чтобы исключить риск одновременного изменения одного и того же объекта несколькими контроллерами доменов и потери модифицированных значений атрибутов.

Это роли *единого гибкого ведущего узла эксплуатации (Flexible Single Master Operations* (FSMO)); при этом каждая из пяти ролей отвечает за определенный аспект функционирования домена или леса. Некоторые из контроллеров домена в роли *единого гибкого ведущего узла эксплуатации,* иногда называемые ведущими узлами, выполняют свою роль в пределах всего домена, так что их действие распространяется на весь данный домен. Если лес состоит из нескольких доменов, каждый домен обладает FSMO-контроллерам и домена, управляющими доменом в целом. Роль других FSMO-контроллеров доменов распространяется на лес в целом. В каждом лесу может быть только один FSMO-контроллер домена, в область действия которого входит лес в целом, независимо от того, сколько доменов содержит лес.

Единый ведущий узел эксплуатации называется *гибким* потому, что эта роль может переходить от одного контроллера домена к другому в пределах домена, если областью действия исходного FSMO-контроллера домена был домен; или между контроллерами других доменов леса, если роль исходного домена распространялась на лес в целом. Однако для такого перемещения роли от вас потребуются некоторые усилия.

Вы назначаете FSMO-роли с помощью утилиты NTDSUTL. Более подробную информацию об утилите NTDSUTL можно найти в справочной системе Windows Server 2003 или в документах Resource Kit.

Приведенный ниже перечень объясняет место каждой из пяти ролей в управлении доменами Active Directory.

- ✓ **Хозяины схемы (Schema master).** *Схема* — это образец для всех объектов и контейнеров, по сути, это сердце Active Directory. Поскольку схема остается неизменной в пределах всего леса, только один контроллер домена можно использовать для модификации схемы. Если контроллер домена, который играет роль хозяина схемы, недостижим, в схему Active Directory нельзя внести никаких изменений. Чтобы вносить изменения в схему, вы должны принадлежать группе администраторов схемы (Schema Administrators Group). (Подробно об определении схемы можно узнать в главе 11.)
- ✓ **Хозяины именования доменов (Domain naming master).** Чтобы добавить домен к лесу, его имя определенно должно быть уникальным. Хозяин именования доменов леса отслеживает операции именования доменов и гарантирует назначение доменам только достоверно уникальных имен. В его функции также входит добавление и удаление перекрестных ссылок на домены из внешних каталогов, таких как каталоги протокола LDAP. Существует только один хозяин именования доменов на лес; вы должны быть членом административной группы предприятия (Enterprise Administrators group), чтобы вносить изменения в правила работы хозяин именования доменов, подобные преобразованию FSMO-роли или добавлению (удалению) домена к лесу.
- ✓ **Хозяин относительных идентификаторов (Relative Ш — RID).** Любой контроллер домена может создавать новые объекты (наподобие пользователей, групп и учетных записей компьютера). Контроллер домена обращается к хозяин RID, когда в его распоряжении остается менее 100 RID. Это значит, что хозяин RID может быть недоступен в течение короткого промежутка времени, что не приводит к проблемам при создании объектов. Это служит гарантией того, что каждый объект обладает уникальным идентификатором (RID). На каждый домен приходится ровно один хозяин RID.

- ✓ Эмулятор **PDC-контроллера.** Контроллер домена-эмулятор PDC работает как основной контроллер домена Windows NT при наличии среды доменов, содержащей BDC-контроллеры Windows NT 4.0 и контроллеры домена Windows 2000 или контроллеры домена Windows 2003 (или и те и другие). Он обрабатывает все изменения паролей Windows NT 4.0, поступающие от клиентов, и тиражирует обновления доменов на BDC-контроллеры более низкого уровня. После завершения модификации на контроллерах доменов и обновления или удаления из среды последнего BDC-контроллера домен Windows 2000 или Windows 2003 (или оба типа доменов) можно переключить для работы в собственном режиме. После перехода домена в собственный режим PDC-эмулятор продолжает выполнять определенные обязанности, с которыми не могут справиться другие контроллеры домена.

  На каждый домен леса, включая дочерние домены, приходится ровно один контроллер домена-эмулятор PDC.
- ✓ **Хозяин** инфраструктуры. Когда пользователь и группа принадлежат разным доменам, может наблюдаться задержка между изменением в профиле пользователя (например, имени пользователя) и его отображением в группе. Хозяин инфраструктуры домена группы отвечает за налаживание связи "группа-пользователь" для отображения события переименования. Хозяин инфраструктуры выполняет согласование локально, а для того, чтобы привести все другие копии объектов домена в актуальное состояние, полагается на тиражирование. (Более подробно тиражирование описывается ниже, в разделе "Как контроллеры доменов работают сообща".)

Доверительные отношения - для доменов Windows NT 4.0 и Active Directory

В старое доброе время, еще до того, как возникла нужда в FSMO-ролях (т.е. в пору расцвета Windows NT), требовался всего один контроллер домена (главный контроллер домена или PDC), который мог вносить изменения в базу данных администратора учетных данных в системе защиты (Security Account Manager — SAM). Эти изменения затем тиражировались на другие резервные контроллеры доменов (BDC). В этой модели база данных SAM представляла собой просто файл, хранимый на каждом PDC-контроллере, который содержал информацию об объектах защиты домена, таких как пользователи и группы. Чтобы поддерживать идентификацию в пределах всего домена (а следовательно, препятствовать несанкционированному доступу к сети), вы создаете односторонние доверительные отношения между доменами, что позволяет пользователям и группам из доверенных доменов назначить доступ к ресурсам домена-доверителя.

Концепция доверителя и доверенного сбивает с толку, поэтому мы постараемся пролить свет на этот предмет. Представьте себе доверительное отношение между двумя доменами: A и B. Домен A "доверяет" домену B, так что домен B является доверенным доменом, а домен A — доменом-доверителем. Поскольку домен A "доверяет" домену B корректно идентифицировать его пользователей, пользователям домена B можно предоставить доступ к ресурсам домена A. (Вы можете создать двухстороннее доверительное отношение, где домен A "доверяет" домену B свои ресурсы, а домен B "доверяет" домену A *свои* ресурсы. Однако в действительности двухсторонняя доверенность не более чем две объединенные односторонние доверенности). Прежде чем вас осенит, что мы все одна счастливая "доверчивая" семья, вспомните, что доверенность на основе Windows NT не обладает свойством транзитивности. Поэтому, если домен C "доверяет" домену B, а домен B "доверяет" домену A, домен C в явном виде не "доверяет" домену A. Что-

бы домен А "доверял" домену С, вы должны установить явное доверительное отношение между доменами А и С. Вы все поняли? Помните об этом, мы вернемся к этим положениям позже.

Когда речь идет о доверительных отношениях, использование Active Directory под управлением Windows Server 2003 оказывается весьма кстати с точки зрения уравнивания доменов в правах. Контроллеры доменов Windows Server 2003 хранят информацию, относящуюся к службе каталогов, в файле (NTDS.DIT), а для идентификации в пределах нескольких доменах по-прежнему необходимы доверительные отношения. Система Windows Server 2003 автоматически создает доверительные отношения между всеми доменами леса так же, как это происходило под управлением Windows 2003, Однако реальное отличие прежней модели доменов Windows NT 4.0 и подхода на основе Active Directory заключается в способе выполнения модификаций и их тиражирования на базу данных доменов. Второе важнейшее отличие состоит в том, что автоматически создаваемые доверенности по умолчанию являются двухсторонними и транзитивными. Теперь если А "доверяет" В, а В "доверяет" С, то А "доверяет" С, — обратное также справедливо.

Не спешите удивляться, вспомните, что Windows 2000 и Windows Server 2003 используют аналогичный подход к доверенностям. Обе операционные системы создают двухсторонние и транзитивные доверенности.

Как контроллеры доменов работают сообща

Во времена Windows NT доменам это было легко делать Вы вносили изменения только на одном контроллере домена, и эти изменения через регулярный интервал копировались на все остальные контроллеры домена.

Теперь, работая с Windows Server 2003, вы можете внести изменения на любом контролере домена и быть уверенным, что "левая рука Windows Server 2003 всегда знает, что делает правая". Вы спросите, как это происходит? Ответ, дорогие друзья, звучит так: тиражирование с несколькими ведущими узлами. (А вы думали, мы скажем "разносятся ветром".) Как именно работает тиражирование с несколькими ведущими узлами, обсуждалось в главе 11, но сейчас мы рассмотрим концепцию на более высоком уровне.

За счет тиражирования с несколькими ведущими узлами любой домен может вносить изменения в базу данных Active Directory. Затем эти изменения тиражируются на все остальные контроллеры этого домена.

В Windows NT конфигурация схемы тиражирования настраивается с использованием пары параметров системного реестра (всего то!) — на самом деле практически бесполезных. В Windows Server 2003 все *намного* круче!

Узел (site) — это совокупность машин и контроллеров домена, соединенных скоростной сетью и сгруппированных в виде IP-подсети. Что должны делать узлы с тиражированием, спрашиваете вы? Да все! Они позволяют нам определять различное расписание для тиражирования в зависимости от состава узла контроллера домена.

Существуют два основных вида тиражирования: *внутриузловое тиражирование (intra-site replication)* (между контроллерами домена одного узла) и *тиражирование (inter-site replication)* (между контроллерами домена разных узлов).

Внутриузловое тиражирование

Когда в Active Directory вносится изменение наподобие добавления или удаления пользователя или изменение атрибута объекта (скажем, добавление свойства к принтеру), это изменение должно быть тиражировано на другие контроллеры домена. Изменение называется *порождающим обновлением (originating update)*. Контроллер домена, где произошло порождающее обновление, посылает уведомление своему партнеру по тиражированию (другому

контроллеру домена узла) о том, что наступило изменение. После выполнения операции тиражирования партнер по тиражированию обладает копией изменения, которое произошло в другом контроллере домена. Это обновление Active Directory партнерского контроллера домена называется *тиражируемым обновлением (replicated update)*, поскольку оно было порождено в другом месте.

Операция тиражирования инициируется между двумя доменами через определенные регулярные интервалы времени (по умолчанию — через пять минут); в то же время существуют ситуации, когда возникает необходимость в срочной операции тиражирования с использованием уведомления. Вот два таких случая.

- ✓ **Тиражирование для одной из вновь заблокированных учетных записей. Предотвращает переход пользователей в другую часть домена, чтобы зарегистрироваться с пользовательской учетной записью, которая заблокирована на контроллере домена.**
- ✓ **Модификация доверительной учетной записи.** Позволяет всем членам домена воспользоваться преимуществами нового доверительного отношения с другим доменом.

Методология тиражирования сталкивается с определенными проблемами. В старое доброе время (иначе говоря, во времена Windows NT 4.0), чтобы избежать проблемы продолжительной задержки в тиражировании новых параметров, нужно было изменить свой пароль на PDC-контроллере. С появлением Windows 2003 изменения пароля сначала вступают в силу на контроллере PDC FSMO; в случае сбоя при установлении пароля контроллер PDC FSMO учитывает ситуацию, когда пароль был только что изменен, но еще не тиражирован.

Если партнеры по тиражированию не получают никаких уведомлений об изменениях в течение часа (этот интервал устанавливается по умолчанию), они инициируют контакт со своими партнерами по тиражированию, чтобы узнать, были ли произведены какие-либо удаленные изменения и были ли утеряны последующие уведомления об изменениях.

Межузловое тиражирование

Межузловое тиражирование осуществляется между определенными серверами одного узла и определенными серверами другого узла. Это звездный час Windows Server 2003. Вы можете настроить расписание тиражирования, в котором задать частоту тиражирования для каждого часа суток. Для этого требуется только выполнить шаги специального программного модуля — оснастки MMC — Active Directory Sites and Services MMC (Start⇨Administrative tool⇨Active Directory Sites and Services). (В русифицированной версии Windows 2000 эти программные модули называются также *оснастками (snap-in). — Прим. ред.)* Перейдите к ветви Inter-Site Transport (Межузловой транспорт) и выберите компонент IP. В правой панели выберите связь с узлом (например, удаленным доменом), щелкните на ней правой кнопкой мыши и выберите элемент Properties (Свойства). Убедитесь в том, что выбрана вкладка General (Общие), а затем щелкните на кнопке Change Schedule (Изменить расписание). Появится диалоговое окно (рис. 12.1), которое используется для изменения времени тиражирования.

Как видно на рис. 12.1, тиражирование назначено на время между 12 и 5 часами пополуночи. Вы можете изменить расписание так, как вам необходимо. Например, вы можете установить время тиражирования между 6 и 7 часами пополудни по воскресеньям.

Для каждой пары узлов можно установить свое время тиражирования. Поэтому в зависимости от характера сетевого взаимодействия и их географического расположения могут подходить разные расписания. Например, если между двумя узлами существует медленный канал глобальной сети, может оказаться необходимым тиражирование с менее частыми обновлениями, чтобы предотвратить перегрузку сети.

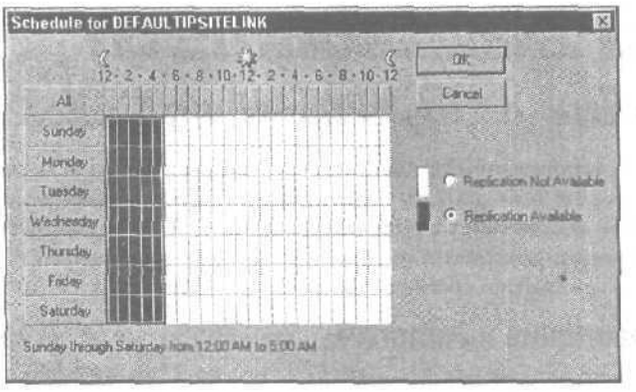


Рис. 12. i. Диалоговое окно для изменения времени тиражирования

Еще одна область тиражирования, которая пересекается с доменами, — это информация глобального каталога (Global Catalog). Глобальный каталог содержит всю информацию обо всех объектах в их собственных доменах и подмножество информации для каждого объекта леса. Однако Windows Server 2003 выполняет все вычисления, необходимые для оптимизации тиражирования, так что вы можете не заботиться об этом.

Пределы вашей базы данных

В Windows 2003 практически не существует ограничений на количество объектов в домене — ваша организация так много просто никогда не создаст! Что касается доменов Windows NT 4.0, то количество объектов ограничено приблизительно 40000 объектов на домен. Это заставляет некоторые компании требовать, чтобы несколько главных доменов объединялись двухсторонними доверительными отношениями.

С другой стороны, Windows 2003 расширяет это количество приблизительно до 1000000 объектов на домен. Компания Compaq провела испытания и создала 16000000 объектов-пользователей в одном домене, не встретив при этом никаких существенных трудностей с производительностью. Однако их оборудование было *очень* мощным — наверное, намного более мощным, чем ваш домашний ПК или даже главный сервер вашей компании!

В определенный момент эти объекты необходимо тиражировать. Windows Server 2003 использует тиражирование *свойств*, а не *объектов,* а это означает, что тиражируются только изменения свойств, а не объекты в целом. Другими словами, если вы изменяете только одно из свойств объекта (например, номер телефона пользователя), тиражируется только изменение свойства (новый телефонный номер), а не объект-пользователь в целом.

Объем вашей базы данных зависит от оборудования вашего контроллера домена и инфраструктуры физической сети. Но если у вас достаточно средств, чтобы вложить их в подходящее аппаратное обеспечение, мы сомневаемся, что вам необходимо больше одного домена (если только ваша компания в действительности не слишком большая). Существуют, однако, другие причины создания нескольких доменов и лесов, например необходимость использования разных схем. (Схемы более подробно рассматривались в главе 11.)

На объем базы данных вашего предприятия может влиять необходимость резервного копирования и восстановления, поскольку вас явно не устроит создание резервной копии, на которое требуется несколько дней.

Желаете администрировать? Управление доменами и каталогами

Если в вашем распоряжении не окажется достаточных средств для управления Active Directory, вы не сможете использовать эту службу на полную мощность. Несмотря на то что Windows Server 2003 поставляется с полным набором готовых средств, вы можете также создавать свои собственные средства и сценарии, используя интерфейс ADSI (Active Directory Scripting Interface — интерфейс программирования сценариев Active Directory).

Консоль управления каталогом

Как и все остальные функции управления в Windows Server 2003, управление Active Directory осуществляется с помощью оснастки MMC (Microsoft Management Console — консоль управления Microsoft). Наиболее часто вам придется прибегать к помощи оснастки Active Directory Users and Computers, окно которой показано на рис. 12.2. Эта оснастка используется для создания и удаления любых объектов (от пользователей до компьютеров), а также управления ими. Она включает некоторые функции устаревшей утилиты User and Server Manager из Windows NT.

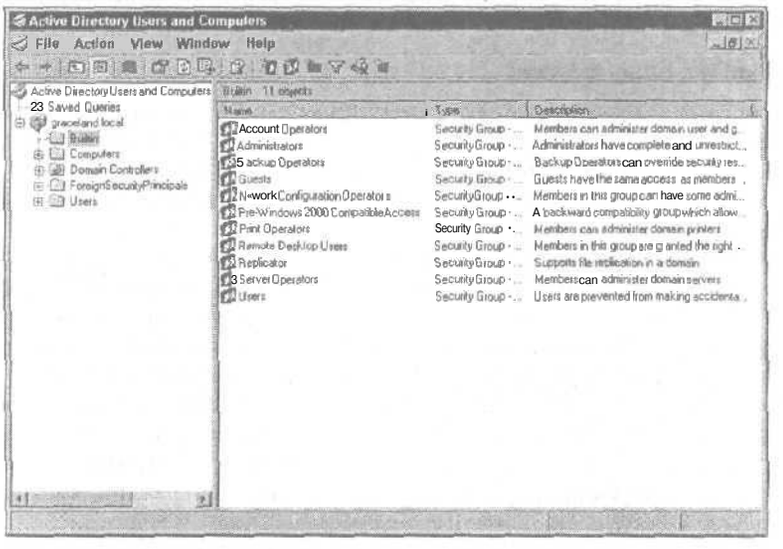


Рис. 12.2. Оснастка MMC Active Directory Users and Computers

Чтобы запустить оснастку Active Directory Users and Computers, выполните команду Start⇨Administrative tool⇨Active Directory Users and Computers (Пуск⇨Администрирование⇨Active Directory: Пользователи и компьютеры). При нервом запуске оснастки в диалоговом окне приложения отображается имя вашего домена (представляемое как DNS-имя домена) в верхней части каталога. Вы можете также заметить несколько контейнеров (более известных как папки). Некоторые из этих контейнеров представляют собой встроенные производственные подразделения предприятия (OU), которые содержат объекты домена, организованные в логические контейнеры, что обеспечивает их лучшее группирование и управление ими в рамках домена. Типичная система Active Directory включает некоторые определенные контейнерные объекты.

- ✓ **Builtin (Встроенный).** По умолчанию содержит детали, относящиеся к описанию прежних групп Windows NT 4.0, такие как Administrators and Backup Operations (Операции администрирования и резервного копирования).
- ✓ **Computers (Компьютеры).** Учетные записи компьютеров, которые управлялись с помощью утилиты Server Manager Windows NT. Объекты-компьютеры других подразделений предприятия не перечислены в этом контейнере.
- ✓ **Domain controllers (Контроллеры домена).** Встроенные подразделения предприятия, которые содержат все контроллеры домена.
- ✓ **Users (Пользователи).** Используемое по умолчанию хранилище для всех пользователей домена. Пользователи других подразделений предприятия здесь не перечислены.

Для полнофункционального домена вы обнаружите здесь различные подразделения предприятия, в зависимости от того, какие службы вы установили и какие подразделения предприятия создали.

Содержимое Windows Server 2003 является *контекстно-управляемым (context driven)*. Это значит, что если вы щелкнете правой кнопкой мыши на объекте или контейнере, отобразится меню, специфическое для данного объекта или контейнера. Это значительно удобнее, чем "охота" за опциями, относящимися к выбранному объекту, в "джунглях" огромных стандартных меню.

Создание объектов каталога

Windows Server 2003 содержит массу объектов, таких как объекты для компьютеров, пользователей, групп и совместно используемых папок. В этом разделе мы рассмотрим создание только двух первых типов объектов (для компьютеров и пользователей), поскольку остальные достаточно интуитивно понятны и не поддерживают многих возможностей конфигурирования.

Применительно к доменам Windows NT планирование создания новых объектов для пользователей или компьютеров никогда не требовало слишком больших усилий. Вы просто создавали их. Однако применительно к Windows Server 2003 подобная непосредственность неуместна. Прежде всего вам следует продумать, где именно вы намерены создавать объекты. Их расположение очень важно, поскольку, несмотря на то, что вы по-прежнему можете перемещать объекты, в долговременной перспективе вам будет намного легче, если вы создадите объекты в подходящем месте с самого начала. Однако, если вы не располагаете достаточным временем на планирование и надлежащее размещение объектов, вы всегда можете позже переместить объекты, куда вам потребуется (просто не говорите, что мы вас не предупреждали).

Использование производственных подразделений (OU) помогает организовать данные в виде логических контейнеров. Первыми вы создаете OU для различных подразделений вашей организации (например, один для бухгалтерии, один для конструкторского отдела, один для отдела кадров и т.д.). Затем вы можете поместить все объекты-пользователи и объекты-компьютеры определенного подразделения в его OU. Кроме того, вы можете облегчить свою административную нагрузку, назначив сотруднику в каждом из подразделений права, необходимые для управления его OU — и только этой OU. Ловко, не правда ли?

Вы можете создать объект-пользователь в двух местах: по умолчанию, в контейнере User/Computer или в некотором производственном подразделении, которое уже создали пользователи или кто-то другой. Если вы делегируете возможность создавать объекты, то можете задать при этом такие ограничения, что пользователи будут способны создавать объекты только в одном месте или в некоторых заданных местах.

Для создания объекта-пользователя выполните следующие действия.

1. **Запустите оснастку Active Directory Users and Computers с помощью команды Start⇨Administrative tool⇨Active Directory Users and Computers.**
2. В диалоговом **окне Active Directory Users and Computers щелкните правой кнопкой мыши на контейнере (таком как Users), в котором вы** желаете создать объект-пользователь, а **затем выберите команду New⇨User (Новый⇨Пользователь).**

   На экране появится первая страница мастера создания пользователя (диалоговое окно New Object — User), как показано на рис. 12.3.

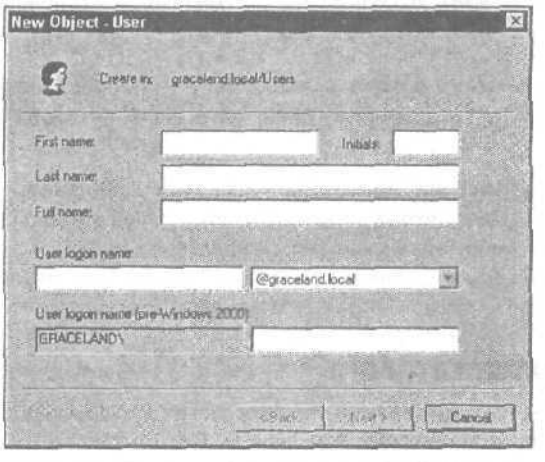


Рис. 12.3. Первая страница мастера создания объектов-пользователей User Creation Wizard

3. **Введите имя пользователя и регистрационное имя пользователя, а затем щелкните на кнопке Next** (Далее).

   Следующая страница мастера позволит вам установить новый пароль и следующие флажки.

   - User must change password at next logon (Потребовать смену пароля при следующем входе в систему).
   - User cannot change password (Запретить смену пароля пользователем).
   - Password never expires (Срок действия пароля не ограничен).
   - Account is disabled (Отключить учетную запись).

4. **Установите подходящие флажки, а затем щелкните на кнопке Next**

   Отобразится итоговое значение добавленных параметров.

5. **Щелкните на кнопке Finish (Готово).**

Ну вот, вы и создали нового пользователя. Вы, наверное, думаете: "А как же все остальные атрибуты пользователя, такие как характеристики безопасности?" Да, вы больше не определяете эти параметры при создании пользователя. После создания объекта-пользователя вы можете щелкнуть на нем правой кнопкой мыши и выбрать пункт меню Properties (Свойства). Появится диалоговое окно Properties для пользователя (рис. 12.4).

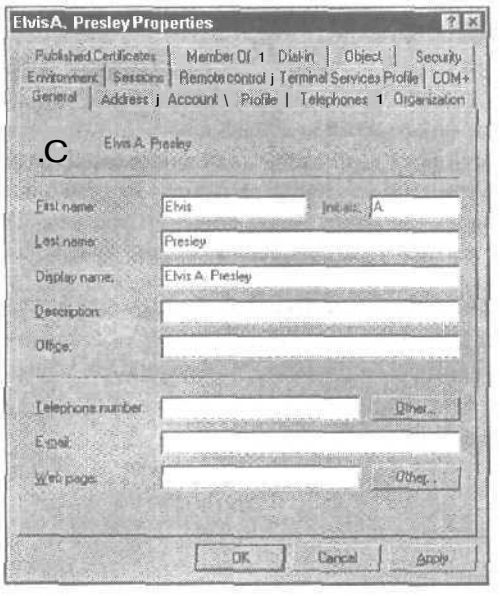


Рис. 12.4. Диалоговое окно свойств для пользователя

Каждая вкладка отображает различные аспекты выбранного объекта-пользователя. Эти вкладки изменяются в зависимости от используемых подсистем Windows Server 2003, других вспомогательных приложений наподобие Exchange Server или SQL Server и даже от того, какое ПО независимых поставщиков вы установили на своем компьютере.

Создание учетной записи компьютера намного легче и не обрушит на вас такое большое количество вкладок. В диалоговом окне Active Directory Users and Computers щелкните правой кнопкой мыши на контейнере, в котором вы желаете создать объект-компьютер, а затем выберите команду New⇨User. На экране появится первая страница мастера создания компьютера (диалоговое окно New Object — Computer), как показано на рис. 12.5. Вам остается только ввести имя компьютера и выбрать, какой пользователь или группа может добавить этот компьютер в домен (User or group).

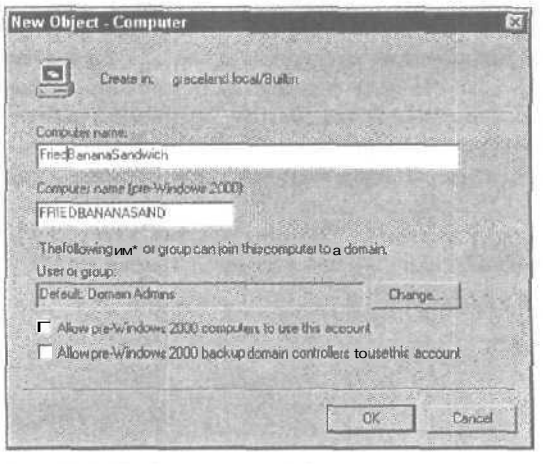


Рис. 12.5. Создание нового объекта-компьютера

Поиск объектов каталога

Возможности поиска объектов — одно из самых больших достоинств Active Directory. Используя глобальный каталог, вы можете отыскать объект в любом месте леса доменов предприятия, запросив информацию у Active Directory.

Вы можете вести поиски любых объектов — пользователей, компьютеров, принтеров, — а также множества атрибутов. (Набор атрибутов зависит от типа объектов, поиск которого вы ведете.) Например, вы можете запросить Active Directory отыскать ближайший на вашем узле принтер с двусторонней цветной печатью. Вам даже нет нужды сообщать Active Directory, где вы находитесь. Он вычисляет это автоматически.

В системе Windows Server 2003 существует компонент Search, доступ к которому можно получить из меню Start (Start⇨Search) (Пуск⇨Поиск). Это меню содержит несколько опций, которые можно использовать для поиска пользователей, папок и принтеров. Вот перечень имеющихся опций.

- ✓ For files and Folders (Файлов и папок).
- ✓ On the Internet (В Internet).
- ✓ Find Printers (Найти принтеры).
- ✓ For People (Людей).

Например, если вам необходимо осуществить поиск цветного принтера, вы можете выбрать команду (Start⇨Search⇨Find Printers) (Пуск⇨Поиск⇨ Найти принтеры). В открывшемся диалоговом окне доступны три вкладки: Printers (Принтеры), Features (Характеристики) и Advanced (Дополнительно). Вы должны выбрать вкладку Advanced, чтобы задать параметры поиска цветного принтера. После ввода всех необходимых деталей щелкните на кнопке Find Now (Найти), после чего на экране отобразится результат поиска. Если вы работаете на большом предприятии, на экране могут отобразиться многочисленные списки принтеров, которые удовлетворяют вашим требованиям, так что всегда старайтесь как можно конкретнее и подробнее указать область поиска.

Несколько слов об ADSI

Интерфейс программирования сценариев Active Directory (или для краткости ADSI) позволяет вам манипулировать службой каталогов с помощью *сценария (script)*. Вы можете использовать сценарии, написанные на таких языках, как Java, Visual Basic, C или C++. С помощью ADSI вы можете написать сценарии, которые автоматически создают пользователей, включая сценарии настройки их параметров, профилей и выбора деталей.

Если вам необходимо управлять средой или большим доменом, вы должны изучить ADSI. В долговременной перспективе это сэкономит вам много времени и сил.

За информацией об ADSI обратитесь на Web-узел `www.microsoft.com/windows/`, и вы найдете массу полезных сведений (больше, чем вам требуется!). Многие подробности можно также найти в документации Windows Server 2003 resource Kit.

Желаете получить разрешение? Работа с fiasfteutetiusiMu для каталогов

Старая концепция "вы администратор, хватит администрировать" в некоторой мере справедлива для Windows Server 2003. Хотя некоторые задания по-прежнему требуют полноценного администрирования доменов, общее управление доменами можно осуществить более легко, если вы наделите различные наборы пользователей правами по управлению разными наборами пользователей и свойствами пользователей. Другими словами, это означает, что вы передаете ответственность за управление низкоуровневыми пользователями пользователям немного более высокого уровня и т.д., до тех пор, пока от вас как администратора не потребуется вмешаться в управление более значимыми компонентами, такими как леса доменов и деревья или межузловой доступ.

Об управлении разрешениями в Active Directory

Если вы знакомы с моделью безопасности Windows NT, вы, возможно, знаете все о *списках контроля доступа (Access Control Lists* — ACL). Список ACL позволяет вам установить разрешения доступа применительно к файлу, каталогу, разделяемому ресурсу или принтеру (и другим объектам) и, таким образом, контролировать множество пользователей, которые могут получать доступ к этим конкретным объектам и модифицировать их.

Система Windows Server 2003 переводит управление разрешениями на новый уровень, связывая ACL-списки с каждым отдельным атрибутом и объектом. Это означает, что вы можете контролировать доступ пользователей на таком уровне, что можете довести подобным "макроуправлением" ваших пользователей до ближайшего сумасшедшего дома. Вы можете, к примеру, потребовать, чтобы "группа пользователей администрирования отдела кадров (Personnel Admin) могла изменять атрибуты адреса, телефонного номера и электронной почты всех пользователей, но ничего более".

Назначение разрешений

Вы можете назначить разрешения на доступ к объектам Active Directory несколькими способами. Здесь мы покажем предельный случай, так что все остальное покажется легче легкого!

Помните утилиту (или оснастку, если хотите) Active Directory Users and Computers? Отлично, ранее в этой главе, в разделе "Консоль управления каталогом", вы получили некоторое представление об этой утилите. Однако она обладает и другими возможностями, которые доступны только в режиме дополнительных возможностей. Чтобы перейти в этот режим, запустите утилиту Active Directory Users and Computers (Start⇨Administrative tool⇨Active Directory Users and Computers), а затем выберите команду View⇨Advanced Features (Вид⇨Дополнительные характеристики).

В корень базового домена добавляются две новые ветви: LostAndFound и System. Впрочем, они нас не интересуют. Нас интересует новая вкладка, которая добавилась к объектам, — Security (Безопасность).

В диалоговом окне утилиты Active Directory Users and Computers найдите любого пользователя. Щелкните правой кнопкой мыши на объекте-пользователе и выберите пункт меню Properties (Свойства). В диалоговом окне Properties для выбранного пользователя щелкните на вкладке Security, а затем на кнопке Advanced (Дополнительно). На экране отобразится список элементов разрешения, состоящих из типа (Allow/Deny (Разрещить/Запретить), имени пользователя или группы, самого разрешения и области его действия (рис. 12.6). Обратите внимание на длину полосы прокрутки...

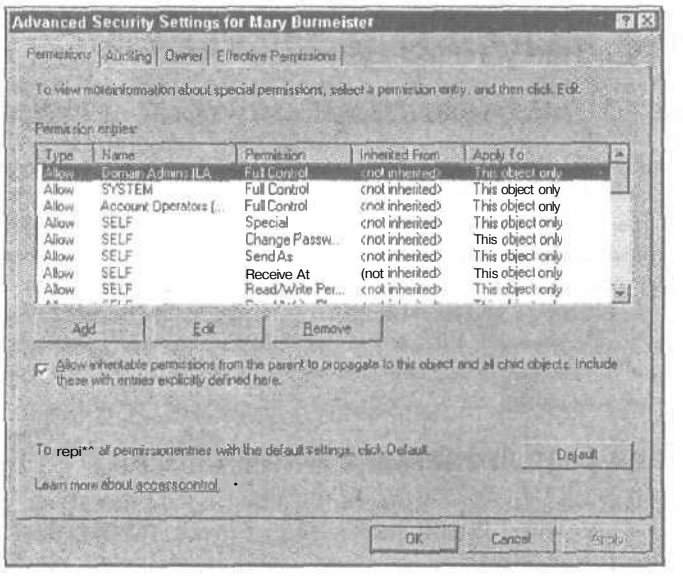


Рис. 12.6. Диалоговое окно Advanced Security Settings для объекта, который используется для контроля доступа пользователей

Очевидно, явное назначение разрешений для каждого объекта займет целую вечность. К счастью, Active Directory использует модель наследования, так что вам необходимо внести изменения только в корень; отсюда изменения распространяются сверху вниз. В следующем разделе объясняется, как это происходит.

Наследование разрешений

Существуют два типа разрешений; явные и наследуемые. *Явные (explicit)* разрешения назначаются непосредственно объекту, а *наследуемые (inherited)* распространяются на объект "по наследству" от его родителя. По умолчанию любой объект контейнера наследует разрешения своего контейнера.

Иногда вам понадобится, чтобы разрешения не наследовались. Например, когда вы работаете со структурой каталога, в которой различные разрешения определяются для каждого содержащегося в ней объекта, как это имеет место в случае узла многопользовательского протокола FTP (File Transfer Protocol — протокол передачи файлов) или разделяемой папки, которая содержит домашние каталоги пользователя. Параметры, используемые в Active Directory по умолчанию, задают наследуемые разрешения, однако вы можете изменить это поведение, подразумеваемое по умолчанию.

Помните вид Advanced Features, который можно получить из окна Active Directory Users and Computers? Так вот, он вам снова потребуется. Когда вы переходите к окну Advanced Features из меню View и отмечаете дополнительные свойства безопасности пользователя (щелкаете правой кнопкой мыши на объекте-пользователе, выбираете Properties, щелкаете на вкладке Security, а затем щелкаете на кнопке Advanced), обратите внимание на маленький флажок Allow Inheritable permissions from parent to propagate to this object and all Child Objects (Переносить наследуемые от родительского объекта разрешения на этот объект и все дочерние объекты). Этот флажок легко пропустить, не правда ли?

По умолчанию флажок Allow Inheritable Permissions From Parent To Propagate To This Object And All Child Objects установлен. Если вы сбросите его, любые изменения, вносимые в родительский контейнер, не будут больше распространяться на объекты, которые он содержит. Вы отключили наследование разрешения для объектов.

Если вы отключили наследование, вам предоставляются следующие возможности.

- ✓ Копировать ранее унаследованные разрешения для этого объекта (Copy previously inherited permissions to this object).
- ✓ Удалить унаследованные разрешения (Remove inherited permissions).
- ✓ Отменить (отключить) наследование (Cancel (disable) the inheritance).

Конечно, вы можете позже включить наследование. Это обратимая операция, так что без паники!

Делегирование административного контроля

Делегирование административных функций определенным элементам вашего домена — одна из самых интересных особенностей Active Directory — нет больше администраторов и не администраторов! Различным людям или группам можно перепоручить контроль над определенными аспектами деятельности подразделения предприятия в рамках домена. Для делегирования административных функций объектам выполните следующие действия.

1. **Щелкните правой кнопкой мыши на контейнере (подразделения предприятия или домена) в окне Active Directory Users and Computers и выберите пункт меню Delegate Control (Передать управление).**

   Откроется окно утилиты Delegation of Control Wizard и отобразится окно приветствия.

2. **Чтобы начать передачу управления, щелкните на кнопке Next.**
3. **Выберите группу пользователей, которым вы желаете делегировать управление.**

   Для этого щелкните на кнопке Add (Добавить), чтобы получить доступ к средствам поиска Active Directory и отыскать необходимых пользователей и группы. Выберите необходимых пользователей и группы (для одновременного выбора нескольких пользователей удерживайте нажатой клавишу <Ctrl>).

   Теперь пользователи отображаются в выбранной пользовательской области. Люди, которых вы выбрали, могут выполнять назначаемые вами задачи.

4. **Щелкните на кнопке Next**

   Отобразится список общих задач, по которым вы можете перепоручить функции управления (например, смена пароля и модификация состава группы).

5. **Выберите необходимые задачи, а затем щелкните на кнопке Next. Если вы выбрали возможность делегирования индивидуальных задач,** следуйте **действиям, которые вам предложит выполнить мастер.**

   Отобразится итоговое окно (рис. 12.7), в котором вы сможете изменить свое решение.

6. **Если вы удовлетворены внесенными изменениями, щелкните на кнопке Finish.**

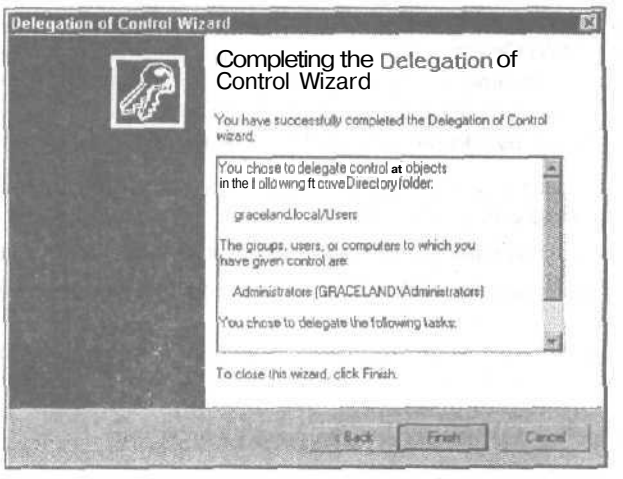


Рис. 12.7. Итоговое окно утилиты Delegation of Control Wizard

Вот и все. Несколько щелчков мышью, и вы делегировали функции управления контейнером определенному лицу или группе людей.

Управление доверительными отношениями

В Windows NT 4.0 управление доверенностями в крупных предприятиях было большой проблемой. Однако в Windows Server 2003 управление доверенностями упростилось благодаря тому, что по умолчанию все доверительные отношения устанавливаются между всеми доменами леса, и эти доверенности представляют собой двусторонние и транзитивные доверительные отношения.

Двусторонние транзитивные доверительные отношения создаются автоматически между всеми доменами леса, когда вы выполняете утилиту DCPROMO. Вы можете, однако, попрежнему создавать "старомодные" доверенности Windows **NT** 4.0 для любого домена, который не является частью того же леса доменов предприятия.

Установление доверительных отношений

Устаревшие доверительные отношения устанавливаются с использованием утилиты Active Directory, доступ к которой можно получить с помощью команды Start⇨Administrative Tools⇨Active Directory Domains and Trusts. Щелкните правой кнопкой мыши на выбранном домене в окне интерфейса утилиты Active Directory Domains and Trusts, а затем выберите пункт меню Properties. Для создания одностороннего доверительного отношения щелкните на вкладке Trusts (Доверие), как показано на рис. 12.8. (Одностороннее доверительное отношение не транзитивно по своей сути и работает так же, как старое доверительное отношение Windows NT 4.0.) Вы можете удалить доверительное отношение, выделив его и выбрав кнопку Remove (Удалить).

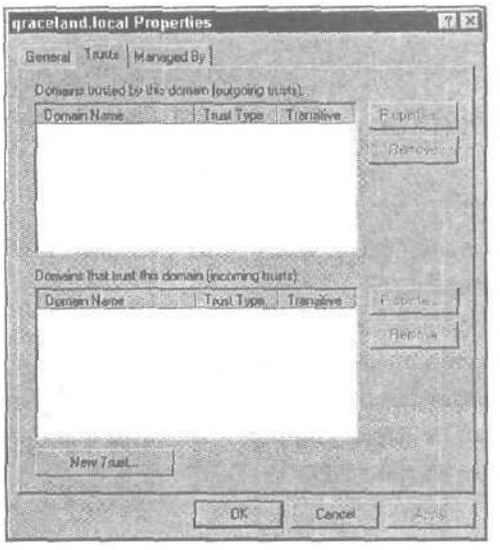


Рис. 12.8. С *помощью этого окна создаются односторонние доверительные отношения между доменами*

Если вы откроете доверчиво дверь, кто сможет пройти внутрь?

При работе с лесом, когда вы открываете "дверь доверия" (что происходит автоматически между всеми доменами одного и того же леса), войти в нее может кто угодно. Все доверенности транзитивны, так что кто угодно в любом из доменов леса может получить разрешение на любой из ресурсов.

Что касается доверительных отношений старого типа (которые создаются вручную между доменами, принадлежащими различным лесам, или доменам Windows NT), то они не транзитивны. Только пользователям в двух доменах, для которых определено доверительное отношение, можно предоставить доступ к ресурсам и только в направлении действия доверенности.

Поэтому, повода для паники нет, поскольку пользователи не могут получить доступ к ресурсам без разрешения. Таким образом, хотя им может быть предоставлен доступ, они не смогут осуществить его до тех пор, пока не получат специально данного им разрешения.

Глава 13

Сетевая печать

В этой главе...

- Способы печати в Windows 2003
- Установка серверной части
- Разделение доступа к устройству печати
- Установка устройства печати на клиентской стороне
- Управление устройствами печати, ориентированными на Windows 2003
- Предупреждение проблем печати
- Управление факсами в Windows 2003

Если нет доступа к сетевым ресурсам, ничто так не тревожит пользователей, как невозможность распечатать свою работу. Бьемся об заклад, что вы не найдете сетевого администратора, который мог бы сказать, что никогда не сражался с устройствами печати.

Мы полагаем, что фирме Microsoft удалось разработать хорошую систему печати для Windows 2003. В этой главе вы познакомитесь с особенностями настройки устройств печати в сети и способами избежать некоторых распространенных проблем печати.

В данной главе мы будем использовать термины Microsoft *устройство печати (print device)* и *принтер (printer),* которые в реальном мире могут сбить с толку. Microsoft определяет устройство печати как физический принтер наподобие HP LaserJet 1200 и принтер — как программное обеспечение на сервере, где вы настраиваете конфигурацию для физического устройства печати. Мы используем термины Microsoft в этой главе, чтобы быть технически точными. Однако если вы никогда не работали с Windows 2003, эта терминология может показаться несколько запутанной.

Модель печати Windows 2003

Когда пользователь печатает свою работу, данные печати проходят определенный путь от пользователя к устройству печати. Схема печати Windows Server 2003 включает следующие основныекомпоненты.

- ✓ Пользователи печати. Это люди, которые желают отправить задание на печать на устройство печати, находящееся сети, в Internet или подключенное к их рабочей станции. В распоряжении пользователя должен быть *драйвер устройства печати (print device driver)* (называемый *драйвером печати,* если не пользоваться терминологией Microsoft), установленный на его рабочей станции.
- ✓ GDI (Graphic Device Interface — интерфейс графических устройств). Расширенный GDI-интерфейс — это программа, которая отыскивает подходящий драйвер устройства печати и работает с драйвером, чтобы перевести информацию печати на подходящий язык принтера. После того как информация переведена, GDI-интерфейс отправляет ее в спулер клиентской части (с точки зрения клиентского приложения Windows GDI — *это процесс печати).*

- **Драйвер устройства печати.** Фрагмент программного обеспечения, который либо поставляется производителем (для самой последней версии), либо компанией Microsoft (не всегда самая последняя) и соответствует определенной марке и модели устройства печати. И вновь, если не пользоваться терминологией Microsoft, это называется *драйвером печати.* Вы могли также слышать название *драйвер принтера.* Драйвер устройства печати не требуется устанавливать непосредственно на клиенте. Если клиент работает под управлением Windows 98/SE/ME/NT/2000/XP, он может загрузить драйвер устройства печати с сервера печати, когда требуется отпечатать документ. Однако это требует, чтобы конфигурация сервера печати предусматривала наличие драйверов устройств печати для этих операционных систем.
- **Принтер.** Называется также *логическим принтером*; это вовсе не физический фрагмент оборудования, который вам иногда хочется ударить, а, скорее, набор установочных параметров, которые вам требуется задать для работы устройства печати. Он существует как программа на сервере, которую вы используете для настройки конфигурации параметров для обработки задания на печать и определения маршрута к физическому устройству печати.
- **Задания на печать (Print job).** Это файлы, которые вам требуется напечатать. Задания на печать форматируются на рабочей станции с помощью GDI и драйвера устройства печати и отправляются для вывода на локальное или сетевое устройство печати. Если устройство печати — локальное (подключено к рабочей станции), результат печатается сразу же. Если в процесс вовлечены сетевое устройство печати и сервер печати, результат отправляется (подкачивается) в очередь на сервере печати, где находится до тех пор, пока устройство печати не освободится для обслуживания запроса.
- **Серверы печати.** Это компьютеры, которые управляют подключенными к ним сетевыми устройствами печати. Сервером печати может быть любой компьютер, расположенный в сети (или в Internet), к которому подключено устройство печати и который работает под управлением некоторой версии операционной системы Microsoft, такой как Windows 2003/2000/NT или Windows 9л. (Даже пользовательская рабочая станция может функционировать как сервер печати — однако нам этот подход не по душе, поскольку обычно он приводит к загрузке пользовательской рабочей станции слишком большим трафиком.) Когда пользователь посылает задание на печать, сервер печати запоминает задание в очереди к устройству печати, а затем опрашивает устройство печати, чтобы проверить, когда оно освободится. Если устройство печати свободно, сервер печати выталкивает очередное задание из очереди и отправляет его на устройство печати.

  Любой сетевой администратор или пользователь с соответствующими правами доступа может управлять сервером печати из любого места сети. По умолчанию в Windows 2003 все члены группы Everyone могут *печатать* на устройстве, однако только члены группы, обладающие особыми правами, *могут управлять* устройством.
- **Очередь печати.** Это место на жестком диске, где закачанные файлы ожидают, когда наступит их черед вывода на устройство печати. С каждым устройством печати связана по меньшей мере одна очередь печати (следовательно, возможны и дополнительные очереди). По мере того как пользователи отправляют задания на печать, последние попадают в очередь, чтобы ожидать печати. Вы определяете очередь для устройства печати, когда добавляете принтер в папку Printers and Faxes и присваиваете ему имя. Задания на печать поступают в очередь по правилу "первым пришел — первым обслужен".

Только тот, кто обладает соответствующими правами на управление очередью (администраторы (Administrators), операторы печати (Print Operators) или операторы сервера (Server Operators)), может изменить порядок печати в очереди печати. Вы можете дать пользователям вашей сети разрешение управлять очередью печати для вас. В системах Windows 2003 имеется встроенная группа под названием Print Operators, и вы можете добавить пользователей в эту группу, чтобы дать им надлежащие права доступа для задачи, с помощью команды Start⇨Administrative Tools⇨Active Directory Users and Computers, а затем выделить домен и открыть папку Builtin (Встроенные).

Предоставление одним пользователям прав управления очередью печати в противовес другим пользователям может выглядеть как политические игры, если вы будете соблюдать чрезвычайную осторожность при назначении прав. Некоторые ребята могут обвинить других в протекционизме, когда задания на печать переупорядочиваются в очереди. Мы часто наблюдали подобную картину. Если вы выберете нейтральных людей, вы облегчите себе жизнь!

- Устройства печатн. Это физические устройства или принтеры наподобие лазерных принтеров от Hewlett-Packard. Вы можете подойти к ним и дотронуться до них. Устройства печати могут быть подключены локально к рабочей станции, или серверу, или непосредственно к сети. В реальном мире (отличном от мира Microsoft), это — то, что мы, обычные люди, называем принтером!

Физические устройства печати

Мы называем устройства печати физическими устройствами печати, поскольку вы можете подойти к ним и дотронуться до них. Существуют различные категории устройств печати, включая лазерные, плоттеры, струйные и термические. Вы можете подключить физическое устройство печати локально к рабочей станции, серверу, серверу печати или непосредственно к сети (рис. 13.1).

Сервер печати — это подключенная к сети рабочая станция, которая обслуживает задания на печать, так что, технически, мы можем отнести рабочие станции и серверы печати к одной категории, В данном случае мы говорим о них отдельно потому, что хотим провести различие между рабочей станцией, где работает пользователь, и специально выделенной рабочей станцией-сервером печати, расположенной в сети.

Логические принтеры

Логическое назначение принтера (logical printer assignment) — не устройство печати, — он существует как нечто неосязаемое в форме определения Windows 2003.

Это нечто наподобие имени, которое Windows 2003 использует для идентификации физического устройства печати (или группы физических устройств печати, как вы увидите позже в этой главе). Всякий раз при определении устройства печати и его свойств в Windows 2003 операционная система назначает определение логического принтера физическому устройству печати, так что она знает, какому физическому устройству печати вы намерены отправить ваше задание.

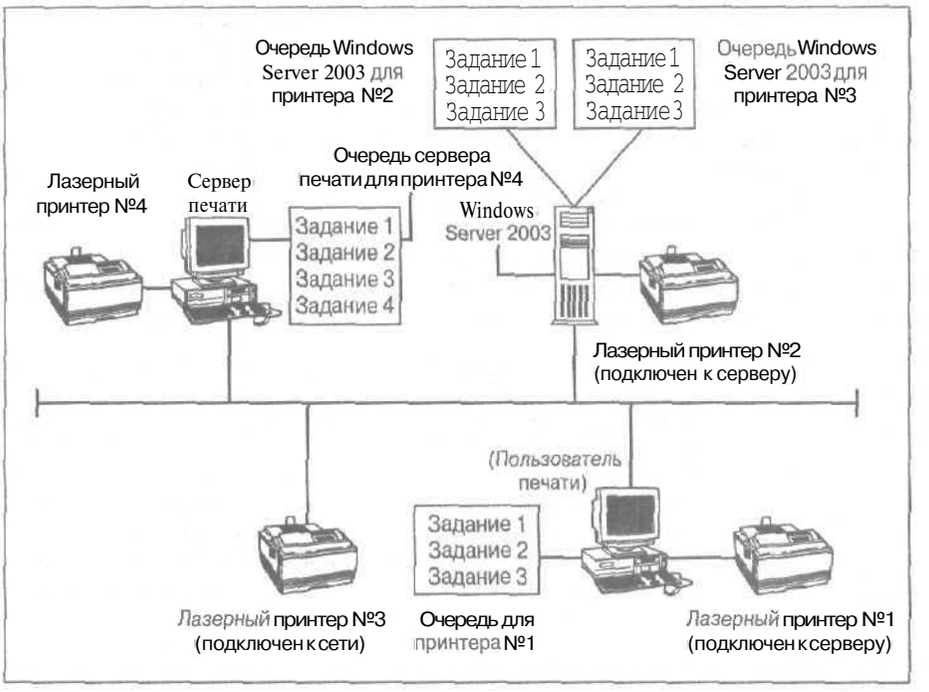


Рис. 13.1. Различные способы подключения устройств печати в сети

При установке устройства печати между физическим устройством печати и логическим определением существует соотношение "один к одному". Однако вы можете расширить использование логического назначения принтера, так что одно логическое назначение принтера служит в качестве определения для нескольких физических устройств печати. Этот способ известен как *организация пула устройств печати (print device pooling)*, и вы устанавливаете его посредством свойств устройства печати, добавляя порт в определение устройства печати.

Вам нет нужды слишком заботиться об определении логических принтеров до тех пор, пока вы не намерены создать пул устройств печати. Это происходит всякий раз, когда вы подключаете устройство печати к серверу (как объясняется ниже, в разделе "Подключение устройств печати к серверам"). Просто следует понимать, что Windows 2003 связывает определение логического принтера с одним или несколькими физическими устройствами печати, подключенными к сети.

Например, вы предпочитаете иметь в своем распоряжении несколько устройств печати, соединенных с вашей сетью, и все (или некоторые) из них принадлежат одному типу наподобие HPLJ1200. Если вы не зададите определения логического принтера для Windows 2003, как система узнает, на какое устройство печати HPLJ1200 посылать ваши задания? Вы обегаете все здание в поисках вашего дорого отчета! Задание определения логического принтера сохраняет порядок в вашем мире. Вы можете назвать один логический притер *2FLWest* и будете знать, что ваш отчет отправлен на принтер HPLJ1200 на втором этаже западного крыла вашего здания.

Еще одна чудесная вещь, с которой вам может помочь логическое назначение принтера, — это достижение сбалансированности заданий на печать. Предположим, что у вас имеются три физических лазерных устройства печати (A, B и C). Если пользователь выбирает отправку зада-

ния на печать на принтер А, который рассчитан на большие по объему задания на печать, значительное время и ресурсы будут потеряны, если принтеры В и С будут простаивать без дела.

Вы можете помочь вашим пользователям в этом отношении, задав одно определение логического принтера и назначив его нескольким различным физическим устройствам печати. Таким образом, ваши пользователи печатают на одном логическом принтере, который затем вычисляет, какое из физических устройств печати свободно. Это позволяет снять принятие решения и беспокойство с пользователя и переложить его на операционную систему. Единственное, чего следует остерегаться в этом случае, — это слишком большого физического расстояния между устройствами печати. Попробуйте убедиться в том, что все физические устройства печати в определении логического принтера находятся в одной общей области, так чтобы пользователям не пришлось бегать по всему зданию в поисках своих распечаток.

Если вы назначаете логическому принтеру обслуживать больше одного физического устройства печати, последние должны быть идентичными. Единственное, что вы можете изменить для каждого устройства печати, — это свойства наподобие номера приемника и размера бумаги.

И, наоборот, вы можете назначить нескольким логическим принтерам обслуживать одно физическое устройство печати. Это может потребоваться, если пользователи печатают специальную продукцию, такую как конверты. Определите функции одного логического принтера как печать с выводом в приемник для конвертов на физическом устройстве печати, а функции другого логического принтера — как печать на стандартной почтовой бумаге на том же устройстве печати.

Если вы присвоите логическому принтеру какое-нибудь описательное имя, пользователи будут знать, где находится устройство печати и какие функции оно выполняет. Например, если назвать два логических принтера *2FLWestEnv* и *2FLWest*, это скажет пользователям, что принтер 2FLWestEnv находится на втором этаже западного крыла и печатает конверты, а другой — обычное устройство печати на втором этаже западного крыла. Оба логических назначения обслуживают одно и то же физическое устройство печати, но должны печатать в разные приемники на устройстве печати, или один может останавливать устройство печати между страницами и т.д. Единственное, что вам при этом необходимо сделать, — определить отдельные устройства печати, которые печатают в один и тот же порт.

Установка серверной части

Прежде чем установить клиентское ПО для печати вашей роботы, позаботьтесь о том, чтобы посетить сервер и установить все определения устройства печати, драйверы и аппаратное обеспечение, а затем переходите к клиентской части. Это служит гарантией того, что когда вы доберетесь до рабочей станции пользователя, вы тотчас же сможете отправить тестовое задание на печать, поскольку все компоненты на месте. Если вы начнете с пользовательской части, вам придется позднее вернуться назад, что выполнить тестирование.

Папка Printer and Faxes

Почти все средства, которые вам необходимы для настройки устройств печати, можно найти на сервере в папке Printers and Faxes (Принтеры и факсы) системной папки Control Panel (Панель управления). (Более быстрый доступ к этой информации можно получить с помощью команды Start⇨Printers and Faxes.) Мы говорим *почти* все, поскольку драйверы устройств печати хранятся вне папки устройств печати. (Большую часть драйверов можно найти на компакт-диске с системой Windows Server 2003.)

Когда вы впервые устанавливаете Windows Server 2003, папка Printers and Faxes содержит только пиктограмму Add Printer (Установка принтера), которая предназначена для того, чтобы помочь вам установить физическое устройство печати (или определение логического принтера). Всякий раз, когда вы устанавливаете новое устройство печати, щелкните мышью на пиктограмме Add Printer (установку мы рассмотрим позже в этой главе). Windows 2003 назначает ему отдельную папку в папке Printers and Faxes (рис. 13.2),

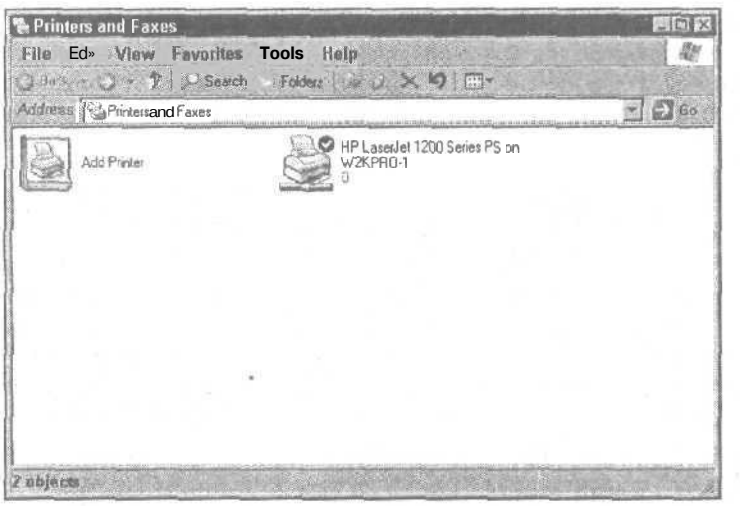


Рис. 13.2. Папка Printers and Faxes, в которой показаны установленное устройство печати и пиктограмма Add Printer

После щелчка на пиктограмме Add Printer появится диалоговое окно мастера установки принтера, содержащее набор применяемых по умолчанию правил, которые используются для того, чтобы провести вас через процесс установки каждого нового устройства печати в папку Printers and Faxes.

После установки требуемого устройства печати вы по-прежнему можете вносить изменения в устройство печати, обращаясь к папке Printers and Faxes. Щелкните правой кнопкой мыши на пиктограмме установленного устройства печати и выберите пункт Properties (Свойства) из выпадающего списка. Появится окно с многочисленными вкладками. Внесите изменения в конкретное устройство печати в этом диалоговом окне Properties и уделите время знакомству с имеющимися установочными параметрами.

Добавление сетевого принтера

В идеальном случае ваша сеть и пользователи позволят вам уставить один тип устройства печати одинаковым способом (наподобие установки всех лазерных устройств печати одной марки и модели с сетевым адаптером). В реальном мире, однако, все не так просто. Поэтому инженеры компании Microsoft создали Windows Server 2003, чтобы обеспечить вам четыре способа подключения устройства печати к вашей сети.

- ✓ Windows Server 2003.
- ✓ Сервер печати.
- V Сетевой (см. рис. 13.1).
- ✓ Рабочая станция.

В следующих разделах мы расскажем о четырех подходах к установке устройств печати в сети. Три из четырех типов установки похожи; они просто выполняются на разных машинах. Например, действия по установке устройства печати, подключенного к сети, и устройства печати, подключенного к рабочей станции, очень похожи. Обе машины обладают устройствами печати, подключенными к их локальному порту, и обе разделяют устройства печати в сети.

Подключение устройств печати к серверам

У вас может возникнуть необходимость подключить устройство печати непосредственно к серверу. Мы не рекомендуем вам использовать этот метод, если только ваша организация не имеет возможности предоставить вам машину, чтобы использовать ее в качестве выделенного сервера печати. Почему? Потому что всякий раз при подключении устройства к серверу вы подвергаетесь риску, что оно может "загнуться" и загубить сервер, — и мы не раз были свидетелями этого.

Чтобы подключить устройство печати к серверу Windows Server 2003, вам необходимы устройство печати, компьютер с установленной системой Windows Server 2003, кабель, инсталляционный компакт-диск Windows Server 2003 (если только вы не скопировали его на жесткий диск компьютера) и все драйверы устройства печати, которые вы желаете загрузить на клиенты.

Соедините устройство печати непосредственно с одним из портов на сервере (например, с LPT1) и установите устройство печати на этой машине в ее папку Printers and Faxes с помощью команды Start⇨Printers and Faxes. Затем выполните следующие действия.

1. **Дважды щелкните на пиктограмме Add Printer, чтобы вызвать мастер-программу установки принтера. Затем щелкните на кнопке Next**
2. **Выберите переключатель Local Printer (Локальный принтер), установите флажок Automatically Detect and Install My Plug and Play Printer (Автоматическое определение и установка принтера Plug and Play), а затем щелкните на кнопке Next**

   На экране отобразится окно New Printer Detection (Поиск нового принтера) и мастер установки принтера отыщет и установит подключенные устройства Plug and Play, Если устройство печати не совместимо со стандартом Plug and Play, следуйте остальным инструкциям, приведенным в этом разделе.
3. **В раскрывающемся списке Use the Following Port (Использовать имеющийся порт) выберите порт, к которому вы подключили это устройство печати (такой как LPT1). Щелкните на кнопке Next**

   В появившемся окне вы можете выбрать производителя и модель устройства печати.
5. **В области Manufacturers (Изготовители) выделите название фирмы-изготовителя устройства печати. В области Printers (Принтеры) выделите модель устройства печати. Щелкните на кнопке Next**

   Если вы не находите свое устройство печати в предлагаемом списке, это значит, что вам необходимо указать мастеру установки принтера на расположение драйвера. Щелкните на кнопке Have Disk (Установить с диска) и укажите мастеру путь к месту расположения драйвера.
6. **В диалоговом окне Name Your Printer (Выберите имя для принтера) мастер установки предлагает имя для этого принтера. Согласитесь с предложенным именем или введите новое имя. Щелкните на кнопке Next.**
7. **В диалоговом окне Printer Sharing (Совместное использование принтера) мастера установки введите имя для этого принтера, если вы предполагаете его совместное использование. Если вы не намерены использовать его как общий ресурс,**

выберите переключатель Do Not Share This Printer (Нет общего доступа). Щелкните на кнопке Next

Общедоступное имя — это имя, которое видят ваши пользователи, когда печатают на этом принтере, так что выберите его так, чтобы оно несло смысловую нагрузку (например, 2ndFLWestEnv, т.е. принтер находится на втором этаже западного крыла и печатает конверты),

7. **В диалоговом окне Location and Comments (Местоположение и комментарий) мастера установки введите местоположение принтера и приведите какой-либо комментарий, касающийся данного устройства печати. (Именно здесь вы можете ввести поясняющую информацию наподобие следующей:** ***2ndFLWestEnv, принтер для печати конвертов, находящийся на втором этаже западного крыла. — Прим. ред.)***

   Ваши пользователи могут воспользоваться этой информацией, когда станут определять, на каком принтере они желают печатать. Чем больше информации вы приведете здесь, тем меньше у вас будет головной боли в будущем!

9. **В предпоследнем диалоговом окне мастер установки предложит вам распечатать пробную страницу** (это **настоятельно рекомендуется делать всегда), а также решить, куда вы желаете установить драйверы для других клиентских операционных систем, которые будут обращаться к принтеру. Щелкните на кнопке Next.**

   Программа установки копирует инсталляционные файлы с компакт-диска Windows 2003 на жесткий диск компьютера, работающего под управлением Windows Server 2003. Также, если на шаге 6 вы решили предоставить принтер для совместного использования, вам необходимо иметь драйверы печати операционной системы для установки (шаг 9), чтобы Windows Server 2003 могла автоматически загрузить драйверы на клиентскую машину.

9. **Если на шаге 8 вы решили установить дополнительные драйверы, программа установки начинает копировать драйверы для этого устройства печати и по необходимости делает паузу, чтобы узнать у вас местоположение и путь к соответствующим драйверам принтера. Введите информацию о пути и щелкните на кнопке OK.**

   Чтобы изменить установленные вами драйверы, вы можете перейти к вкладке Sharing (Доступ) диалогового окна Properties (Свойства). Более подробная информация приведена ниже, в разделе "Управление устройствами печати, ориентированными на Windows 2003".

10. **Если вы решили не печатать пробную страницу и не устанавливать дополнительные драйверы, программа установки отобразит страницу с итоговой информацией о выбранных вами параметрах. Если установленные вами параметры верны, щелкните на кнопке Finish (Готово). В противном случае воспользуйтесь кнопками Back (Назад) и Next** (Далее) **для корректировки информации.**

Если вы знакомы с процедурой установки принтеров по предыдущим версиям Windows, вы быстро пройдете через эти шаги, поскольку установка устройств печати похожа. К этому моменту вы выполнили следующие установки.

- ✓ **Одно назначение базового логического принтера, которое указывает на одно физическое устройство печати в системе Windows Server 2003.** Мы говорим базовое, поскольку вы пока еще не задали для устройства печати параметры, подобные типу приемника для бумаги, количеству точек на дюйм и разделителю страниц. Ве-

роятно, вы еще не знали о том, что при определении этого физического устройства печати вы также назначаете ему логический принтер. Помните о том, что всякий раз, когда вы устанавливаете физическое устройство и определяете его, до тех пор, пока вы не добавили дополнительные физические устройства, между этими двумя устройствами (физическим и его логическим определением) существует соотношение "один к одному".

- ✓ Очередь печати для этого устройства печати. Эту очередь устанавливает для вас Windows 2003, когда вы определяете устройства печати. Для просмотра очереди дважды щелкните на пиктограмме устройства печати. Вы пока еще ничего не увидите в очереди.
- ✓ **Общий доступ к данному устройству печати для всех, кто подключен к сети.** Когда вы определяете для устройства печати общедоступное имя в сети, Windows 2003 по умолчанию назначает группе Everyone доступ к этому устройству печати. Если вы не желаете, чтобы "кто угодно" имел доступ к этому устройству печати, вы должны изменить это применяемое по умолчанию правило. Если в вашей системе установлена Active Directory, устройство печати будет опубликовано в каталоге.

Несколько назначений логических принтеров может указывать на одно физическое устройства печати. Если вам необходимо определить другое назначение логического принтера, который обслуживает это физическое устройство печати, вы повторяете предыдущие шаги, но назначаете новый компьютер и общедоступное имя. Вы можете назначить этому физическому устройству печати разные свойства для каждого определения логического принтера.

Подключение устройств печати к серверам печати

В предыдущем разделе мы рассказали, как подключить устройство печати к компьютеру, работающему под управлением Windows Server 2003. Так что ваша система Windows Server 2003 в дополнение к своим обычным обязанностям функционирует еще и как сервер печати в вашей сети. Чтобы справиться с нагрузкой на сервер Windows Server 2003, вы можете разгрузить его, передав эти задания на печать другому компьютеру в вашей сети и заставить *его* функционировать в качестве сервера печати.

Сервер печати — это еще один компьютер в сети с подключенным к нему устройством печати, который вы устанавливаете для управления подкачкой данных печати, очередями печати и заданиями на печать. Мы предпочитаем этот метод, поскольку он освобождает Windows Server 2003 для выполнения других задач. Когда ваши клиенты печатают посредством сервера печати, они минуют сервер Windows Server 2003.

На компьютер, который будет вашим принтером печати, вы можете установить любую операционную систему Microsoft. Мы рекомендуем устанавливать по меньшей мере Windows *9x,* но предпочтительнее рабочие станции под управлением Windows NT/2000 или Windows XP, поскольку в этом случае вы можете загрузить драйверы принтеров на клиентские рабочие станции автоматически с сервера печати. Это означает, что вам нет необходимости устанавливать драйверы вручную на каждой рабочей станции.

После установки операционной системы на вашем предполагаемом сервере печати повторите шаги 1-10 из раздела "Подключение устройств печати к серверам", если вы используете в качестве операционной системы Windows NT/2000 шш Windows XP Workstation. Если вы используете Windows *9x,* выполните те же действия за исключением определения загружаемых драйверов устройств печати (шаги 8 и 9). Вместо этого вам необходимо установить на каждой клиентской машине соответствующие драйверы устройств печати.

Подключение сетевых устройств печати к серверам печати

Некоторые устройства печати, такие как лазерные принтеры от Hewlett-Packard, хорошо подготовлены, и, после того как вы вставите в них карту сетевого адаптера, они почти готовы к тому, чтобы их поместили в любом месте сети, где имеется электрическая розетка и свободное сетевое соединение. Почти, да не совсем! Вам еще необходимо установить все физические соединения и назначить принтеру IP-адрес. После этого выполните следующие действия, чтобы добавить сетевой принтер к серверу печати.

1. **Щелкните на папке Printers and Faxes.**

   Отобразится окно Printers and Faxes.

2. **Дважды щелкните на пиктограмме Add Printer для вызова мастера установки принтера, затем щелкните на кнопке Next.**

3. **В диалоговом окне Local and Network Printers (Локальный или сетевой принтер) установите переключатель Local Printer Attached to This Computer (Локальный принтер, подключенный к этому компьютеру) и снимите флажок Automatically Detect and Install My Plug and Play Printer, а затем щелкните на кнопке Next**

   На экране появится следующее диалоговое окно мастера установки.

4. **В диалоговом окне Select the Printer Port (Выберите порт принтера) щелкните на переключателе Create a New Port (Создать новый порт). Выберите из раскрывающегося списка Type of Port (Тип порта) элемент Standard TCP/IP Port Щелкните на кнопке Next**

   Отобразится диалоговое окно Welcome to the Add Standard TCP/IP Printer Port Wizard (Добро пожаловать в мастер установки стандартного порта TCP/IP принтера).

5. **Щелкните на кнопке Next.**

   Отобразится диалоговое окно Add Port (Установка порта).

6. **В диалоговом окне Add Port введите IP-адрес сетевого устройства печати и дайте порту имя. Мастер установки подставит имя за вас, но при желании вы сможете изменить его. Щелкните на кнопке Next.**

   Если ваше устройство печати правильно сконфигурировано и установлено и вы ввели верную информацию в диалоговые окна мастера установки, он поместит ваше устройство в сеть и отобразит информацию о нем.

7. **Для завершения установки щелкните на кнопке Finish.**

При установке принтера в системе Windows Server 2003 с инсталлированной службой Active Directory мастер установки определяет ваше устройство печати как общий ресурс и публикует его в каталоге — если только вы не измените правила политики. За более подробной информацией об Active Directory обратитесь к главе 11.

Подключение устройств печати к рабочей станции

На рабочем столе у некоторых пользователей имеются устройства печати, которые вы намерены сделать доступными другим пользователям сети. Подключение устройства печати к рабочей станции — наименее желательный способ, поскольку заставляет пользователей ходить к рабочим станциям других пользователей, чтобы "ловить" свои задания на печать. Это может нарушить рабочий процесс у тех пользователей, которые имеют несчастье держать устройства печати на своих столах. Однако в небольших организациях, где бюджет ограничен, этот метод используется.

Вам необходимо войти на рабочий стол рабочей станции пользователя и установить для этого устройства печати статус общего сетевого ресурса. Вы можете ограничить доступ к этому общему ресурсу, так что вся организация не сможет здесь печатать. Где вы сможете найти средства, чтобы реализовать все это? Конечно, в папке Printers and Faxes на рабочем столе пользователя! Если ни одно устройство печати не установлено, щелкните правой кнопкой мыши на пиктограмме Add Printer, выберите устройство печати, которое должно быть локальным устройством печати, подключенным к порту LPT1, и присвойте ему имя. Если устройство печати уже определено, щелкните правой кнопкой мыши на пиктограмме устройства печати и выберите пункт меню Properties, чтобы присвоить этому устройства печати общедоступное имя. После того как вы передадите устройство печати для совместного использования в сети, другие пользователи смогут увидеть его.

Этот метод приводит к тому, что процессом печати управляет рабочая станция пользователя. Вы можете определить это подключенное к рабочей станции устройство печати таким образом, что процессом печати будет управлять сервер Windows Server 2003.

1. **Войдите на рабочий стол компьютера пользователя и определите для этого устройства печати статус совместно используемого ресурса, но ограничьте доступ к нему только именем пользователя "JoePrinter".**

   Чтобы узнать, как определить общий ресурс, обратитесь к следующему разделу "Разделение доступа к печати".

2. **Вернитесь назад к Windows Server 2003.**
3. **В диалоговом окне Active Directory Users and Computers (Пользователи и компьютеры Active Directory) добавьте пользователя с именем "JoePrinter" (Start⇨Administrative Tools⇨Active Directory Users and Computers (Пуск⇨Администрирование⇨Active Directory — Пользователи и компьютеры).**
4. **В папке Printers and Faxes дважды щелкните на пиктограмме Add Printer.**
5. **Следуйте инструкциям, приведенным выше, в разделе "Подключение устройств печати к серверам", за исключением следующего.**
   - Щелкните на пиктограмме Add Printer и выберите сетевое устройство печати вместо локально подключенного устройства печати (My Computer (Мой компьютер)).
   - Щелкните на переключателе Type the Printer Name or Click Next to Browse for the Printer (Введите имя принтера или щелкните на кнопке "Далее" для обзора принтеров). Либо введите имя общего ресурса, либо воспользуйтесь кнопкой обзора для выделения и выбора имени общего ресурса, которое вы дали устройству печати на клиентском рабочем столе.
   - Дайте устройству печати новое имя общего ресурса, которое будут видеть остальные пользователи сети.

Мы не рекомендуем использовать этот метод, только если ваша организация не ограничена в средствах. Он может ухудшить положение тех пользователей, которые должны разделять устройства печати с другими пользователями сети и может разрушить их рабочую среду,

Совместный доступ к принтерам

После того как вы установили принтер в сети, следующий шаг состоит в создании совместно используемого сетевого ресурса для этого устройства печати. (За более подробной информацией о совместно используемых ресурсах сети Windows Server 2003 обратитесь к главе 16.)

До тех пор, пока вы не назначите устройству печати статус совместно используемого ресурса, ваши пользователи не увидят его в сети. Чтобы сделать устройство печати общим ресурсом, выполните следующие действия.

1. **Откройте папку Printers and Faxes (Start⇨Printers and Faxes).**
2. **Щелкните правой кнопкой мыши на пиктограмме устройства печати, которое вы желаете сделать общим ресурсом, и выберите вкладку Sharing** (Доступ).
3. **Во вкладке Sharing выберите переключатель Share This Printer (Использовать совместно этот принтер) и введите описательное имя совместно используемого ресурса (например, 2ndFLWest).**
4. **Если вы желаете, чтобы этот принтер попал в список Active directory, установите флажок List in the Directory (Включить в каталог).**
5. **Щелкните на кнопке OK, и процедура завершена!**

Если в вашей сети имеются клиенты, которые работают под управлением MS DOS, убедитесь в том, что имена совместно используемых устройств печати состоят не больше чем из восьми символов.

Объединение принтеров и клиентов

Завершающий шаг установки сетевых принтеров состоит в установке устройств печати на стороне клиентов. К счастью, этот процесс требует немногого. Все, что вам необходимо, имеется в системе Windows Server 2003, на сервере печати или на рабочем столе пользователя в папке Printers and Faxes, в зависимости от того, какая клиентская операционная система используется.

Если клиентская ОС — это Windows XP/2000 или NT, вам необходимо только установить устройство печати в диалоговом окне Printers and Faxes (Add Printer) и выбрать опцию Networked Print Device (Сетевое устройство печати). Причина в том, что устройство печати подключено к другому компьютеру где-то в сети; он не является локальным для этой рабочей станции. Для порта используйте кнопку Browse и найдите общедоступное имя устройства печати, на котором вы намерены печатать. Вот и все!

Если ваши клиенты работают под управлением Windows *9x* и печатают на Windows Server 2003 (и вы установили на сервере драйверы разных клиентских ОС), вы просто устанавливаете устройство печати в диалоговом окне Printers and Faxes (Add Printer) и выбираете его в качестве сетевого устройства печати. Когда вы выбираете порт как общедоступное имя сетевого устройства печати, Windows Server 2003 автоматически загружает драйверы.

Управление принтерами, ориентированными на Windows 2003

Вы можете управлять вашими серверами печати, очередями и устройствами печати из любого места сети, включая ваш сервер Windows Server 2003. Из одного места сети вы можете просматривать, что происходит со всеми устройствами печати в вашей сети. Единственное, что вы не можете сделать в удаленном режиме, — это что-нибудь установить на самом устройстве печати, например память или кабели. Но об этом вы уже знаете!

Ниже перечислены некоторые вопросы, которые необходимо иметь в виду при управлении устройствами печати.

- **Дисковое** пространство на **сервере.** Если вы устанавливаете в сети функцию подкачки (спулинга), вам необходимо пристально следить за дисковым пространством на сервере печати. Процесс подкачки включает отправку файлов от пользователя печати на сервер печати. Помните, что сервер печати может также быть вашим сервером Windows Server 2003. В противном случае, если сеть отличается высоким уровнем объема печати, процесс подкачки может довольно быстро заполнить ваш жесткий диск.

  После подкачки файлов на сервер печати они остаются на жестком диске в очереди до тех пор, пока не освободится устройство печати. Если с устройством печати возникнет проблема, работы могут быстро накапливаться. Помните, что очереди занимают место на жестком диске, так что если очереди накапливаются, требуется все больше и больше дискового пространства. Следите за тем, чтобы дисковая память не исчерпалась совсем.

- **Память устройства печати.** Когда сетевые пользователи печатают графические изображения, память становится критическим параметром устройства печати. Для печати больших графических файлов требуется больше памяти. Вы можете определить объем памяти устройства печати, проверив устройства печати. У некоторых организаций бюджет не настолько велик, чтобы они могли позволить себе покупку дополнительной памяти на все сетевые устройства печати, поэтому они выбирают одну или несколько стратегических точек сети, а затем определяют настройки логического устройства печати таким образом, что они указывают на хорошо оснащенные принтеры.

- **Настройка свойств принтера.** Чтобы получить доступ к меню свойств принтера, щелкните правой кнопкой мыши на пиктограмме устройства печати в папке Printers and Faxes. (На рис. 13.3 показаны различные параметры, которые вы можете изменить для любого устройства печати в сети.) Мы пройдем по всем вкладкам, чтобы вы поняли, какие свойства устройства печати вы можете изменить.

  - General (Общие). На эту вкладку вы добавляете информацию об устройстве печати, такую как комментарии, местоположение, а также принимаете решение о том, использовать ли баннерную страницу. (Поле команды печати, в которое помещается описание текста, пересылаемого на принтер, для использования в качестве заголовка задания на печать. — *Прим.ред.)* Мы рекомендуем вам добавить некоторые общие комментарии, касающиеся устройства печати, а также сведения о его местоположении. В средних и больших организациях целесообразно добавить страницу-разделитель, чтобы задания на печать было легче отделять одно от другого. Здесь же можно найти информацию об установленном драйвере. Эту информацию следует изменять только в том случае, если вы устанавливаете новый драйвер.

  - **Sharing (Доступ).** Если вы желаете, чтобы пользователи сети видели это устройство печати, определите здесь общедоступное содержательное имя. Вы также можете проинструктировать Windows 2003, чтобы это устройство появилось в каталоге. Здесь же вы сообщаете Windows 2003 о том, какая клиентская ОС установлена в вашей сети и для какой системы вы желаете автоматически подгрузить драйверы.

  - Ports (Порты). Здесь вы сообщаете системе о том, к какому порту подключено ваше устройство печати. Если это устройство печати подключено непосредственно к сети, вы определяете его на этой вкладке с помощью MAC-адреса (Media Access Control — протокол управления доступом); если это устройство печати работает с протоколом TCP/IP, вы определяете его, указав IP-адрес.

- **Advanced (Дополнительно).** Вы можете выполнять задания на печать для данного устройства печати ночью. На этой вкладке вы можете задать расписание загрузки устройства печати, приоритет заданий на печать и возможности подкачки,
- **Security (Безопасность).** Здесь вы можете задать возможности аудита устройства печати, которые позволят вам собирать информацию о том, все ли в порядке с принтером. Вы можете использовать вкладку Security, чтобы установить систему оплаты на уровне подразделений (при этом вы следите за использованием принтера и назначаете пользователям или подразделению плату за это использование) или для ограничения доступности устройства печати. Вы можете также определить, кто будет управлять этим устройством печати.
- **Device Settings (Параметры устройства).** Здесь вы определяете специальные свойства устройства печати, такие как размер бумаги, количество точек на дюйм и приемник для бумаги.

Рис. ***13.3.*** *Вкладка* ***Properties*** *устройства печати в папке* ***Printers and Faxes***

Предупреждение проблем печати

Последствия возникновения проблем сетевой печати могут быть разрушительными. Ниже приведено несколько полезных рекомендаций о том, как воспрепятствовать этим проблемам, Некоторые полезные советы приведены также в главе 22.

- **Приобретайте HCL-совместимые устройства.** Приобретайте только устройства печати, перечисленные в списке HCL от Microsoft (Hardware Compatibility List — перечень совместимого оборудования). В противном случае вы можете потратить очень много времени в попытках заставить устройство печати работать в сети — и в результате обнаружить, что устройство просто несовместимо, И никогда не забывайте посещать Web-узел Microsoft, чтобы узнать о последней версии HCL.

- ✓ **Приобретайте последние версии драйвера.** Убедитесь в том, что вы получаете последний драйвер устройства печати для каждого устройства печати в сети. В новых драйверах устранены ошибки, обнаруженные в предыдущих версиях. Если вы используете старый драйвер, это может закончиться поиском известной ошибки, которая уже исправлена в новом драйвере.
- ✓ **Покупайте известные марки.** Мы надеемся, что ваша организация в состоянии позволить себе купить для сети устройства печати известных марок, например Hewlett-Packard и Epson. Мы обнаружили, что наибольшие проблемы с печатью в сети вызваны дешевыми моделями. Иногда на то, чтобы добиться работы от всех собранных вместе дешевых компонентов, тратится столько времени, что разумнее все-таки вложить средства в устройства печати известных марок.
- ✓ **Приобретайте устройства одного изготовителя.** По возможности мы придерживаемся одного типа (марки) устройств печати. Заметьте, мы сказали *марки, а* не *модели.* Мы понимаем, что некоторым организациям необходима печать как черно-белая, так и цветная. Если вы можете приобрести все устройства печати у одного изготовителя (например, Hewlett-Packard), вы облегчите жизнь себе и своим пользователям. Если в вашей сети установлены только лазерные устройства печати от Hewlett-Packard, не покупайте лазерные устройства печати другого изготовителя только потому, что они в это день распродавались в ближайшем компьютерном супермаркете. Вы можете сэкономить время, работая с одним поставщиком, его оборудованием и его драйверами, вместо того, чтобы рыскать по Web-узлам изготовителей в Internet. Позвольте вашим пользователям хорошо узнать одну марку, и им не придется все время учиться использовать новое оборудование.
- ✓ **Купите достаточно памяти.** Наступление графического ПО оказывает большую нагрузку на использование памяти устройствами печати для получения желаемого результата. Не дожидайтесь, пока задания на печать начнут отказывать из-за отсутствия дополнительной памяти. Если ваш бюджет не позволяет вам сделать это заранее, найдите местного поставщика, у которого в запасе имеется память для компьютера, и держите номер его телефона под рукой.

Способы работы с факсами в Windows 2003

Windows 2003, так же как и Windows XP, включает собственную поддержку факсимильной связи. Это значит, что вы можете отправлять и принимать факсы, используя компьютер без ПО от сторонних поставщиков. Возможности Windows 2003 по работе с факсами управляются посредством (вы угадали) папки Printers and Faxes.

Работа с факсимильной аппаратурой не разрешена по умолчанию. Во-первых, в вашем распоряжении должен быть уже установленный и правильно сконфигурированный факс-модем (это значит, что драйверы установлены и все функционирует как следует). Во-вторых, чтобы включить возможности работы с факсами, следует открыть папку Printers and Faxes из меню Start или Control Panel и выбрать команду File⇨Set Up Faxing (Файл⇨Установка факса). Запустится мастер установки факса и установит необходимые компоненты для работы с факсами. Спустя несколько секунд вы вернетесь в папку Printers and Faxes, где появится новая пиктограмма факса.

Команда Properties (Свойства) для пиктограммы факса открывает диалоговое окно со множеством вкладок, очень похожее на диалоговое окно свойств принтера. В этом диалоговом окне вы можете выполнить следующие действия.

- ✓ Определить имя факсимильного аппарата и его местоположение.
- ✓ Определить факсимильный аппарат как совместно используемый сетевой ресурс.
- ✓ Определить доступ и управление защитой.
- ✓ Установить функцию отслеживания документов.

В действительности работа с факсом напоминает печать, но вместо отправки задания на печать документа на физическое устройство печати, где результат выводится на бумагу, задание на печать подвергается оцифровке и отправляется по телефонной линии принимающему факсимильному аппарату (который может быть традиционным факсимильным аппаратом или выполняющим его роль компьютером). Помимо указанного телефонного номера и наличия титульной страницы, факсимильный документ во многом похож на документ, отпечатанный на принтере. Для отправки факса выберите факсимильный аппарат из списка принтеров в диалоговом окне, которое появится после выбора команды File⇨Print (Файл⇨Печать).

При первой попытке отправить факс появится мастер настройки факса, который используется для задания информации о вашей факс-системе, такой как телефонный номер, региональный код и отправитель информации.

Дважды щелкните мышью на пиктограмме факса, чтобы открыть консоль факса (Fax Console), которая используется для того, чтобы отслеживать и управлять входящими и исходящими факсами, во многом аналогично тому, как вы управляете электронной почтой в Outlook. Если вы желаете изменить информацию об отправителе, выберите команду Tools⇨Configure Fax from the Fax Console. Для приема факсов вам следует разрешить входящие факсы и установить ответ после контроля схемы.

Помните, что на каждый модем может приходиться только одна служба ответа. Поэтому, если вам необходимо принять вызов дистанционного пользователя для подключения к вашей сети, не устанавливайте для этого модема функцию ожидания факсов. Устройство, ожидающее входящие факсимильные сообщения, может по-прежнему использоваться для отправки факсов или для обычного коммутируемого соединения. Если вы обнаружите, что нуждаетесь в большей помощи, касающейся возможностей факсов в Windows 2003, обратитесь к справочной системе и документации Windows Server 2003 Resource Kit.

Глава 14

IP-адресация

В этой главе...

- Работа с именами TCP/IP и NetBIOS
- IP-адресация, сети и подсети
- Получение IP-адресов для Internet
- Использование частных IP-адресов
- Использование proxy-серверов и трансляции адресов
- Работа со службой DHCP
- Выявление и устранение проблем

Стек протоколов TCP/IP *(Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Internet)* управляет Internet и позволяет пользоваться им по всему миру. Однако TCP/IP — много больше, чем просто набор протоколов: многие элементы TCP/IP привязаны к протоколам соответствующих служб, что обеспечивает значительно более полные возможности. К наиболее значительным примерам относятся динамическое распределение и управление адресами, известное как служба DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации узлов), а также имена доменов для службы разрешения адресов, известной как служба имен доменов (Domain Name System — DNS). В этой главе вы узнаете об именах и адресах TCP/IP, о соответствующих стандартных службах, а также о некоторых других связанных с ними службах, которыми оснащено семейство ОС Windows Server 2003.

Преобразование имен: TCP/IP и NetBIOS

Применение команды Windows Server 2003 предполагает использование соответствующего синтаксиса. В противном случае ваши усилия не приведут к желаемому результату. Например, когда вы вводите в приглашение командной строки команду NET USE, вы должны вести имя сервера и имя совместно используемого ресурса, равно как и диск, на который вы желаете отобразить сервер. Поэтому простая команда наподобие

```
NET USE G: \\LANWRIGHTS\APPS
```

связывает букву диска G с именем совместно используемого ресурса APPS на сервере LANWRIGHTS. Если вы используете протокол TCP/IP для передачи необходимых данных, протокол не знает, как интерпретировать имя LANWRIGHTS в качестве имени сервера, зато он понимает IP-адреса, например 172.16.1.7.

Если вы используете в сети протокол TCP/IP, вам необходим некоторый способ преобразования IP-адресов в имена и наоборот. Точно так же как в ООН требуются переводчики, чтобы все участники заседаний могли понимать друг друга, для Windows 2003 также требуются "переводчики", вот почему знание соглашений об именах и методов разрешения имен в адреса составляет важную часть работы с протоколом TCP/IP в Windows Server 2003.

Имена NetBIOS

При слове *NetBIOS* вас, как, впрочем, и большинство людей, охватит чувство легкой паники. Не нужно волноваться. Только немногие действительно понимают NetBIOS в деталях, поэтому понять, что вам действительно необходимо знать, совсем несложно.

NetBIOS-имя часто называют *компьютерным именем*. При установке Windows Server 2003 в сети каждый компьютер, работающий под управлением Windows 2003, требует уникального компьютерного имени. Это позволяет всем ориентированным на NetBIOS утилитам идентифицировать каждую машину по ее имени. Когда вы вводите команду, содержащую имя компьютера, Windows 2003 знает, о каком компьютере идет речь.

Если вы попробуете дать двум устройствам одно и то же имя, вы столкнетесь с проблемой, — это то же самое, как попытаться использовать один и тот же идентификационный код для двух людей. Всякий раз, когда компьютер соединяется с сетью, она регистрирует его имя с помощью службы просмотра или службы броузера (browser services), которая следит за подобными вещами. Когда другой компьютер с таким же именем попытается зарегистрироваться, попытка отвергается, поскольку имя уже занято. В действительности этой машине будет запрещено соединиться с сетью до тех пор, пока ее имя не будет изменено на другое, уникальное.

При создании NetBIOS-имен вам необходимо придерживаться принятых для них ограничений.

- ✓ NetBIOS-имена могут содержать не больше 15 символов. (Если в вашей сети имеются машины, работающие под управлением DOS Windows *3.x,* они не распознают NetBIOS-имена, которые состоят более чем из 8 символов.)
- ✓ NetBIOS-имена не должны содержать следующие символы:

  " (знак двойных кавычек);
  / (косая);
  \ (обратная косая);
  [(левая квадратная скобка);
  ] (правая квадратная скобка);
  : (двоеточие);
  ; (точка с запятой);
  | (вертикальная черта);
  = (знак равенства);
  + (знак "плюс");
  * ("звездочка");
  ? (вопросительный знак);
  < (открывающая угловая скобка);
  > (закрывающая угловая скобка).

  Кроме того, не рекомендуется использовать знак доллара, поскольку он обладает специфическим значением. (NetBIOS-имя, в конце которого стоит символ $, не появится в списке броузера.)
- ✓ Не используйте длинные имена и не вставляйте в них пробелы. Windows 2003 не заботится о том, превышаете ли вы допустимую длину имен или не включаете ли в них пробелы, но другие сетевые клиенты или системы могут не справиться с подобной ситуацией.
- ✓ Выбирайте мена, которые несут смысловую нагрузку, достаточно короткие и меткие. Не называете машины по имени их пользователя или местоположению, особенно

если пользовали приходят и уходят, а машины многократно перемешаются с места на место. Для серверов подбирайте такие имена, чтобы отразить их организационную роль или принадлежность группе (отделу) (например, Sales (Сбыт), Accounting (Бухгалтерия) или Engineering (Конструкторский)).

Каким же должно быть это NetBIOS-имя, спросите вы? NetBIOS-имя должно кратко и ясно указывать на обозначаемый предмет, чтобы пользователи могли понять, что перед ними. В лучшем случае этот вид соглашения об именовании имеет смысл без дальнейших объяснений. Вы можете сделать то, что делаем мы: прикрепите наклейку с именем машины на корпус каждого компьютера для идентификации. Вы можете просмотреть список ваших сетевых NetBIOS-имен, раскрыв раздел My Network Places (Мое сетевое окружение) Windows Explorer. Примерный список NetBIOS-имен, заимствованный из нашей сети, показан на рис. 14.1 (таких как W2kpro-1 и W2kpro-2).

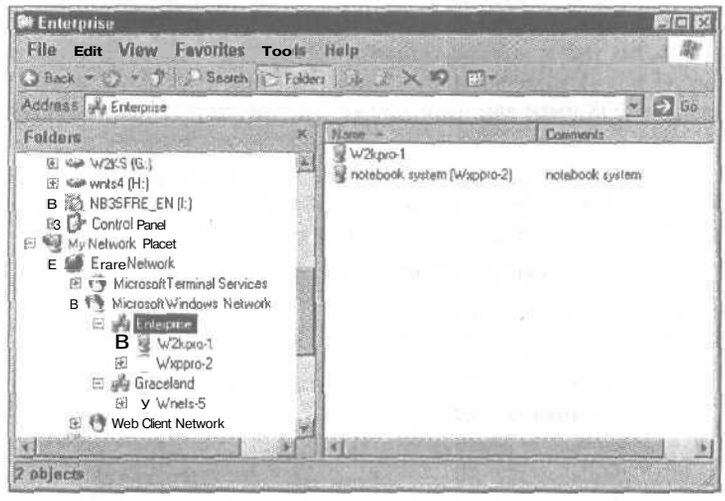


Рис. 14.1. NetBIOS-имена компьютеров в нашей сети

Имена и адреса TCP/IP

Протокол TCP/IP использует схему для имен, отличную от схемы имен NetBIOS. Для создания IP-адресов TCP/IP использует 32-разрядные числа (например, 172.16.1.11). Каждая хост-машина или узел в сети TCP/IP должны обладать уникальным IP-адресом.

IP-адреса не о чем не говорят большинству людей и трудны для запоминания. Поэтому полезно пользоваться каким-нибудь правилом для преобразования IP-адресов в осмысленные имена. В сети Windows Server 2003 вы используете имена компьютеров (также известные как имена NetBIOS). Internet-сообщество использует другое соглашение об именах, называемое именами доменов. Методы трансляции имен, реализуемые такими службами, как WINS (Windows Internet Naming Service — служба имен Internet для Windows) и DNS (Domain Name System — служба имен доменов), поддерживают базы данных для преобразования ГР-адресов в имена компьютеров (WINS) или доменов (DNS).

Если вам приходилось пользоваться Web-броузером в Internet, вы знаете, что можете ввести URL (Uniform Resource Locator — унифицированный указатель информационного ресурса), например `www.lanw.com/`, или IP-адрес (`206.224.65.194/`), чтобы получить доступ к Web-странице. Это возможно благодаря тому, что Internet использует службу DNS для пре-

образования IP-адресов в доменные имена и наоборот. Если вы введете IP-адрес, Web-броузер сразу перейдет по этому адресу; если вы введете имя домена, ваш запрос пройдет через DNS-сервер, который преобразовывает имя в IP-адрес, а затем Web-броузер переходит по этому адресу.

В мире IP-адресов, если вы планируете подключить сеть непосредственно к Internet, на схему именования, которую вы можете применить, накладываются ограничения. VeriSign (www.verisign.com) — одно из многих бюро регистрации имен доменов, которые отвечают за согласование и сопровождение базы данных "законных" имен доменов Internet верхнего уровня. Вы можете запросить любое имя, какое пожелаете, но если кто-то другой использует его или имеет законные притязания на торговую марку или товарный знак, вы не сможете использовать его. Например, вы, скоре всего, не сможете использовать в качестве доменных такие имена, как mcdonalds.com или cocacola.com. Или, если кто-либо другой уже зарегистрировал имя xyzcorp.com, вы не сможете использовать это имя, даже если компания называется "корпорация XYZ".

Типичное IP-имя имеет следующий формат: *хост-имя.имя-домена.суффикс*. Конечно, вы не можете полностью за это ручаться, но обычно имя домена представляет вашу организацию. Суффикс, называемый именем *домена верхнего уровня (top-level domain),* иногда идентифицирует страну (например, суффикс .ca обозначает Канаду (Canada), .de — Германию (Germany)) или тип организации (.gov обозначает правительственную организацию (government), .edu — образовательную (education), .com — коммерческое предприятие (commercial), .org — некоммерческую организацию (organization) и т.д.).

Некоторые имена доменов более сложные и могут иметь следующий вид: *хост-имя.субдомен.имя-домена.суффикс*, как, например, в случае jello.eng.sun.com, где jello — хост-имя; eng — имя субдомена (для конструкторского подразделения — engineering); sun (имя домена для корпорации Sun Microsystems) — имя домена, который представляет коммерческую (.com) организацию. Различные организации, регистрирующие имена доменов Internet (наподобие VeriSign и других компаний и организаций, которые можно найти на Web-странице www.norid.no/domenenavnbaser/domreg.htm), контролируют только такие части имени, как имя домена и суффикс, — каждое доменное имя должно быть полностью уникальным, чтобы его можно было верно распознать.

Имя, которое включает хост-часть, имя домена и суффикс (а также любую другую допустимую информацию о субдомене), называется *полностью определенным именем домена (Fully Qualified Domain Name — FQDN).* Любое допустимое FQDN-имя должно обладать соответствующим элементом в базе данных некоторого DNS-сервера, что позволяет транслировать его в уникальный числовой IP-адрес, Например, наш Web-сервер именуется www.lanw.com и превращается в IP-адрес 206.224.65.194.

До тех пор, пока вы полностью изолированы от Internet и намерены сохранить такое положение дел, вы можете назначать в пределах своей сети любые имена и IP-адреса по своему усмотрению. Однако, как только вы подключаете сеть к Internet, вам придется вернуться и все исправить! Если ваша сеть будет — или, *может, когда-нибудь будет* — подключена к Internet, у вас есть две возможности назначения адресов.

- ✓ **Вы можете сразу получить и установить общедоступные IP-адреса и имена доменов.**

  В этом вам поможет поставщик услуг Internet. Когда вы получите диапазон IP-адресов для сети — помните, каждый компьютер нуждается в своем собственном уникальном адресе, а некоторые компьютеры и устройства нуждаются в нескольких адресах (по одному на каждый интерфейс), — удостоверьтесь в том, что вы получили их достаточно, чтобы оставить некоторый резерв для роста.

✓ **Вы можете (и должны) получить допустимое имя домена от VeriSign или другого регистратора имен доменов, но вы можете использовать и любой диапазон зарезервированных IP-адресов, называемых частными IP-адресами, для нумерации вашей сети.**

Эти адреса могут не использоваться непосредственно в Internet; они могут быть установлены отдельно для частного использования. При использовании с определенным видом ПО под названием NAT (Network Address Translation — трансляция сетевых адресов) этот подход требует от вас получения только небольшого количества общедоступных IP-адресов, но по-прежнему обеспечивает возможность доступа к Internet для каждого компьютера вашей сети. Более подробно эта тема обсуждается ниже, в разделе "Трансляция адресов: еще один фокус".

Чтобы узнать больше о способе получения имен доменов, посетите Web-узел корпорации VeriSign по адресу `www.verisign.com`. На главной странице можно найти форму для поиска имен доменов (позволяющую определить, используется ли уже где-либо подобное FQDN-имя) и регистрации доменных имен (применительно к новым FQDN-именам). Здесь вы найдете подробности, касающиеся служб регистрации имен, а также служб каталога и базы данных, которые поддерживают распределенный по всей Internet набор DNS-служб.

Перекличка всех узлов

Уникальный числовой идентификационный дескриптор, называемый *IP-адресом*, присваивается каждому интерфейсу в сети TCP/IP. Каждый IP-адрес в сети TCP/IP должен быть уникальным. Каждое устройство в сети TCP/IP известно как *хост* (*host*). Каждый хост обладает по меньшей мере одним сетевым интерфейсом с присвоенным ему IP-адресом. Однако хост может иметь несколько карт сетевого интерфейса и несколько IP-адресов, назначенных каждому из интерфейсов.

Сетевой или хост-идентификатор

IP-адрес состоит из двух компонентов: сетевого и хост-идентификатора. *Сетевой идентификатор* указывает сетевой сегмент, к которому принадлежит хост. *Хост-идентификатор* указывает отдельный хост в определенном сетевом сегменте. Хост-узел может непосредственно взаимодействовать только с другими хостами внутри того же сетевого сегмента *Сетевой сегмент (network segment)* — это логическое подразделение сети в рамках уникального числового идентификатора, называемого *подсетью* (*subnet*). Чтобы взаимодействовать с хостами внутри другой подсети, хост должен использовать маршрутизатор.

Маршрутизатор перемещает пакеты из одной подсети в другую. Кроме того, он зачитывает сетевой идентификатор для адреса назначения пакета и определяет, должен ли пакет остаться в текущей подсети или будет перенаправлен в другую подсеть. После того как маршрутизатор доставит пакет в надлежащую подсеть, он использует хост-часть идентификатора адреса назначения для доставки пакета в его конечный пункт назначения.

Типичный IP-адрес выглядит так:

```
207.46.249.222
```

(Данный IP-адрес соответствует имени домена `www.microsoft.com`.) Этот числовой формат IP-адреса известен как *десятичное представление с разделительными точками* (*dotteddecimal notation)*. Однако компьютеры "видят" IP-адреса как двоичные числа. Этот же IP-адрес в двоичной форме выглядит как

```
1100111 00101110 1111001 11011110
```

и записывается наборами по восемь бит, называемыми *октетами*. Каждый октет преобразуется в десятичное число, а затем разделяется точками, образуя формат десятичного представления с разделительными точками, как показано выше.

Вариант IP-адреса в десятичном представлении с разделительными точками в большей мере подходит для восприятия человеком, чем двоичный вариант. Как вы, возможно, уже знаете, имена доменов и NetBIOS-имена еще более удобны в этом отношении, поскольку используют символические имена, которые несут определенный смысл.

IP-адрес требует 32-разрядных чисел и определяет 32-разрядное адресное пространство, которое поддерживает около 4,3 миллиарда уникальных адресов. Хотя это кажется огромным количеством адресов, количество доступных IP-адресов быстро сокращается. Поэтому существует несколько планов по расширению и изменению схемы IP-адресации, которые призваны обеспечить значительно большее количество доступных адресов. Более подробно об этих планах можно узнать на Web-узле IPng Transition, воспользовавшись для этого программой поиска.

Разработчики IP-протокола разделили всю "галактику" IP-адресов на классы, каждый из которых предназначен для удовлетворения специфических потребностей в адресации. На сегодняшний день существуют пять классов IP-адресов, обозначаемых буквами от A до E. Классы A, B и C присваиваются организациям, чтобы обеспечить подключение их сетей к Internet, а классы D и E зарезервированы для специальных целей.

Первые три класса адресов различаются по тому, как определяются их сетевые идентификаторы.

- ✓ Адреса класса A используют для представления идентификатора сети первый октет.
- ✓ Адреса класса B используют первые два октета.
- ✓ Адреса класса C используют первые три октета.

Адреса класса A поддерживают сравнительно небольшое количество сетей, каждая из которых обладает огромным количеством возможных хостов. Адреса класса C поддерживают огромное количество сетей, каждая из которых содержит относительно небольшое количество хостов (табл. 14.1). Класс B занимает промежуточное положение. Поэтому отделения военных и правительственных агентств и крупных корпораций предпочитают использовать адреса класса A; средним по размерам организациям и компаниям необходимы адреса класса B; небольшим компаниям и организациям требуются адреса класса C.

Таблица 14.1. Классы адресов и соответствующие идентификаторы сети и хоста

Класс	Старшие биты	Первый диапазон октета	Количество сетей	Количество хостов
Класс A	0xxxxxxx	1-126.x.y.z	126	16777214
Класс B	10xxxxxx	128-191.x.y,z	16384	65534
Класс C	110xxxxx	192-223.x.y.z	2097152	254

Если речь идет о распознавании адресов классов A–C, то первый октет идентификатора сети для класса A всегда начинается с числа 0. Первый октет любого идентификатора сети класса B начинается с числа 10, а идентификатор сети класса C — с числа 110. Поэтому вы можете определить классы адресов, изучив адрес либо в двоичном, либо в десятичном преставлении (табл. 14.1 и 14.2).

Идентификатор сети под номером 127 пропущен в табл. 14.1, поскольку это идентификатор адреса обратной связи. *Адреса обратной связи (loopback addresses)* используются при испытании передачи по протоколу IP — они осуществляют передачу на самих себя.

Таблица 14.2. **Деление** октетов компонентов IP-адресов в соответствии с классами

Класс	IP-адрес	Идентификатор сети	Идентификатор хоста
A	10.1.1.10	10	1.1.10
B	172.16.1.10	172.16	1.10
C	192.168,1.10	192.168.1	10

Введение подсетей: время покоя для IP-адресов

Подсети представляют подразделение единого адреса сети TCP/IP между логическими подсетями. Существуют две причины создания подсетей. Во-первых, введение подсетей снижает общий объем трафика через любой сегмент сети за счет объединения в группы систем, которые часто взаимодействуют между собой. Во-вторых, введение подсетей облегчает процесс роста и расширения сетей и, кроме того, добавляет дополнительный уровень контроля их безопасности. Подсети работают за счет "захвата" нескольких разрядов из хост-части IP-адреса и использования этих разрядов для разделения единого IP-адреса между двумя или более подсетями.

Маршрутизаторы перемещают пакеты между подсетями и сетями

В мире сетей TCP/IP только маршрутизаторы способны передать пакеты из одной подсети в другую или от одного идентификатора сети к другому. Маршрутизаторы — это специализированные, высокотехнологичные и высокоскоростные устройства, изготавливаемые такими компаниями, как Cisco Systems и Bay Networks. Любой компьютер, оснащенный двумя и более сетевыми адаптерами, может выступать в роли маршрутизатора только в том случае, если компьютер может переадресовывать пакеты с одного адаптера «а другой (и, таким образом, из одной подсети в другую). И здесь весьма кстати оказывается, что Windows 2003 включает ПО и встроенные возможности для функционирования в качестве маршрутизатора. Компьютерные фанаты предпочитают называть такие машины многодомными ***компьютерами*** (***multi-homed computers***), поскольку такие машины чувствуют себя "как дома" в двух и более подсетях.

Для разделения блоков IP-адресов на подсети меньшего размера сетевые администраторы обычно используют маски подсетей. *Маска подсети (subnet mask)* — это специальный двоичный шаблон, который заимствует хост-часть IP-адреса и позволяет разделить большую сеть на две или несколько подсетей, каждая из которых обладает своим собственным уникальным адресом. Базовые маски подсети для сетей классов A–C имеют вид 255.0.0.0, 255.255.0.0 255.255.255.0 соответственно. Вы можете создать дополнительные маски подсетей, добавив дополнительные единичные разряды на занимаемое нулевым разрядом, который появляется сразу за самым правым блоком 255 в любом таком числе. Это преобразование, а также некоторые типичные значения для допустимых масок подсетей показаны в табл. 14.3.

Таблица 14.3. Маски и данные подсетей

Двоичная маска	Десятичный эквивалент	Количество новых подсетей	Количество хостов
00000000	A: 255.0.0.0	A: 16777214	1
	B: 255.255.0.0	B: 65534	
	C: 255.255.255.0	C: 254	
10000000	A: 255.128.0.0	A: неприменимо	Неприменимо

Окончание табл. 14.3

Двоичная маска	Десятичный эквивалент	Количество новых подсетей	Количество хостов
	B: 255,255.128.0	B: неприменимо	
	C: 255.255.255.128	C; неприменимо	
11000000	A: 255.192.0.0	A: 4194302	2
	B: 255.255,192.0	B: 15382	
	C: 255.255.255.192	C: 62	
11100000	A: 255.224.0.0	A: 2097150	6
	B: 255.255.224.0	B: 8190	
	C: 255.255.255.224	C: 30	
11110000	A: 255.240.0.0	A: 1048574	14
	B: 255.255.240.0	B: 4094	
	C: 255.255.255.240	C: 14	
11111000	A; 255.248.0.0	A: 524286	30
	B: 255.255,248,0	B: 2046	
	C: 255.255.255.248	C: 6	
11111100	A: 255.252.0.0	A: 262142	62
	B;255.255.252.0	B: 1022	
	C:255.255.255.252	C; 2	
11111110	A: 255.254.0.0	A; 131070	126
	B: 255.255.254.0	B; 510	
	C: 255.255.255.254	C: неприменимо	

Поскольку маршрутизации требуются для взаимодействия в рамках IP-подсетей, некоторые IP-адреса маршрутизаторов в каждой подсети должны быть известны всем клиентам этой подсети. Этот адрес называется *шлюзом по умолчанию (default gateway),* поскольку именно сюда направляются все внешние по отношению к подсети передачи. (Другими словами, это шлюз для всего остального мира сетей, лежащего за пределами локальной подсети.) Если шлюз по умолчанию не определен, клиенты не могут взаимодействовать за пределами своей подсети.

Повесьте вывеску: получение IP-адреса Internet

Развертывание собственной сети или использование автономной системы с ПО трансляции сетевых адресов (NAT) для подключения к Internet требует получения одного или нескольких IP-адресов. В некоторых случаях вы можете просто заключить контракт с поставщиком услуг Internet (ISP) для использования коммутируемого соединения. При каждом соединении вам автоматически назначается IP-адрес из пула доступных адресов. После разрыва соединения с ISP этот IP-адрес возвращается в пул для повторного использования. Этот метод в равной мере хорошо работает для автономных машин и серверов, которые должны устанавливать автоматическую связь с ISP для обеспечения соединения по запросу пользователей, которые обладают частными IP-адресами, но могут соединиться с Internet, используя программное обеспечение **NAT.**

Один из способов подключения всей сети к Internet состоит в том, чтобы арендовать блок, или подсеть, IP-адресов у ISP. Однако аренда IP-адресов может дорого обойтись и ограничить рост вашей сети. Также многие ISP могут не сдавать в аренду крупные блоки IP-адресов, так что доступ ваших определенных машин или подсетей к Internet может быть ограничен.

Чтобы узнать больше об этом подходе, свяжитесь со своим ISP, чтобы выяснить, что он может предложить в качестве доступных адресов или непрерывных блоков IP-адресов для подсетей. В некоторых случаях необходимы общедоступные IP-адреса, поскольку обеспечение безопасности требует установления истинного сквозного соединения между клиентами и серверами через Internet. Попросту говоря, истинное сквозное соединение (end-to-end connection) означает, что IP-адрес, о котором клиент извещает Internet, соответствует тому, который он в действительности использует. Ниже, в разделе "Трансляция адресов: еще один фокус", вы познакомитесь с альтернативным подходом, при котором IP-адрес, объявляемый в Internet, отличается от частного IP-адреса, который клиент использует в своей подсети.

Для некоторых приложений, в особенности тех, где требуется безопасный IP-ориентированный протокол наподобие IP Secure (IPSec) или конкретная реализация протокола защищенных сокетов (Secure Sockets Layer — SSL), методы трансляции сетевых адресов могут не работать! Убедитесь в том, что вы понимаете требования вашего приложения в подробностях, прежде чем примите решение о том, арендовать ли общедоступные IP-адреса или использовать частные IP-адреса с трансляцией сетевых адресов.

Трансляция адресов: еще один фокус

Если вы не желаете платить за аренду диапазона IP-адресов и ваше приложение позволяет вам использовать частные IP-адреса, вы можете воспользоваться IP-адресами, зарезервированными для частного использования в RFC 1918 в сети. (RFC (Requests for Comments) — запросы на комментарии, серия документов проблемной группы проектирования Internet (Internet Engineering Task Force — IETF), появившаяся в 1969 году и содержащая описания набора протоколов Internet и связанную с ними информацию. — *Прим.ред.)* При использовании с ПО трансляции сетевых адресов для соединения с ISP все, что вам требуется для обслуживания всей сети, — это один общедоступный IP-адрес (или один — для каждого Internet-соединения).

Документ RFC 1918 (который можно найти на Web-странице `www.fags.org/rfcs/rfcs1918.html`) определяет специальные IP-адреса для использования в частных intranet-сетях. Эти адреса, приведенные в табл. 4.4, по определению не подлежат маршрутизации в Internet. В дополнение подобный подход обеспечивает более высокий уровень безопасности сетей, поскольку любой мошенник, который намеревается проникнуть в вашу сеть, не сможет легко замаскироваться под локальную рабочую станцию. (Чтобы добиться этого, потребуется маршрутизировать пакет с частным IP-адресом через Internet.) Поскольку все подобные адреса — общедоступны, вы можете использовать класс адресов, который подходит вашей организации (вы можете использовать столько адресов класса B и C, сколько вам необходимо, в пределах допустимого диапазона таких адресов).

Таблица 14.4. Диапазоны частных IP-адресов из RFC1918

Класс	Диапазон адресов	Номер сети
A	10.0.0.0-10.255.255.255	1
B	172.16.0.0-172.31.255.255	16
C	192.168.0.0-192.168.255.255	254

Использование ПО трансляции адресов в качестве попытки обеспечить доступ к Internet снижает затраты и позволяет обеспечить практически неограниченный рост сети. Если вы считаете, что частные IP-адреса в сочетании с ПО NAT имеют смысл в вашей ситуации, проконсультируйтесь у вашего ISP по поводу конкретных деталей, касающихся применения этой технологии в вашей сети.

Если вы читали статьи или книги, в которых говорится о доступе к Internet, то, вероятно, встречали термины *брандмауэры (firewall)* и *proxy*. Брандмауэры и proxy-серверы — это сетевые средства, которые представляют собой нечто чуть большее, чем специализированные маршрутизаторы. Брандмауэр можно использовать для фильтрации трафика — как входящего, так и исходящего.

Фильтры брандмауэров могут базироваться как на адресе отправителя, так и на адресе получателя, на специфическом протоколе или адресе порта или на шаблоне, который может появляться в пакете данных. *Proxy-сервер* — это усовершенствованный брандмауэр, целью которого является управление взаимодействием внутренней сети и внешних сетей наподобие Internet. Proxy-сервер скрывает идентичность внутренних клиентов и может хранить локальные копии часто запрашиваемых ресурсов (это называется *кешированием (caching)* и уменьшает время отклика для пользователей).

В Internet существует несколько отличных источников информации о брандмауэрах; однако информация о proxy-серверах ограничена документацией на продукты. Помимо справок, которые можно получить в документации Resource Kit для Windows Server 2003 и на Web-узле TechNet (www.microsoft.com/technet/default.asp), существует несколько Internet-ресурсов, к которым вы можете обратиться, чтобы узнать больше об этих технологиях.

- ✓ Great Circle Associates (www.greatcircle.com).
- ✓ Internet Security and Acceleration Server (ISA) компании Microsoft (www.microsoft.com/isaserver).
- ✓ Виртуальная частная сеть (VPN) компании Aventail (www.aventail.com).
- ✓ Zone-Alarm компании Zone Lab (www.zonealarm.com).
- ✓ PIX Firewall компании Cisco (www.cisco.com/univercd/cc/td/doc/pcat/fw.htm).
- ✓ WinProxy компании Ositis Software (www.ositis.com).
- ✓ WinGate Pro компании Deerfield Communication (www.deerfield.com).

Помимо этих великолепных продуктов от сторонних поставщиков Windows Server 2003 обеспечивает встроенный собственный продукт-брандмауэр, известный как Internet Connection Firewall, который можно включить и сконфигурировать с помощью вкладки Advanced (Дополнительно) объекта соединения. Брандмауэр IFC может обеспечить базовую защиту, однако он не обладает многосторонностью и возможностями, которых требует от брандмауэра производственная сеть. Если вы желаете больше узнать о IFC, обратитесь к таким источникам, как Help-система, Support Center и Resource Kit Windows Server 2003.

Как заставить Windows Server 2003 "проглотить" TCP/IP

Настройка конфигурации протокола TCP/IP в Windows 2003 может быть простой и сложной. Мы рассматриваем простой процесс и обсуждаем лишь отдельные более сложные вопросы. Чтобы ознакомиться с настройкой сложной конфигурации, обратитесь к справочным пособиям Resource Kit Windows Server 2003 или TechNet.

Для настройки конфигурации протокола TCP/IP всегда требуются три элемента.

- ✓ IP-адрес.
- ✓ Маска подсети.
- ✓ Шлюз по умолчанию,

Именно эти три элемента позволяют вам подключить клиента или сервер к сети. Настройка конфигурации протокола осуществляется в диалоговом окне Internet Protocol (TCP/IP) Properties. Чтобы получить доступ к этому диалоговому окну, выполните следующие действия.

1. **Выберите команду Start⇨Control Panel⇨Network Connection⇨Local Area Connection (Пуск⇨Панель управления⇨Сетевое подключение⇨Подключение по локальной сети)**
2. **Щелкните на кнопке Properties (Свойства).**

   Появится диалоговое окно Local Area Connection Properties (Свойства подключения клокальной сети).
3. **В списке установленных КОМПОНЕНТОВ выберите Internet Protocol (TCP/IP).**
4. **Щелкните на кнопке Properties, чтобы открыть диалоговое окно Internet Protocol (TCP/IP) Properties.**

Если протокол TCP/IP еще не установлен, выполните следующее.

1. **В диалоговом окне Local Area Connection Properties щелкните на кнопке Install (Установить).**

   Появится диалоговое окно Network Component Type (Тип сетевого компонента).
2. **Выберите переключатель Protocol, а затем щелкните на кнопке Add (Установить).**

   Появится диалоговое окно Select Network Protocol (Выбрать сетевой протокол).

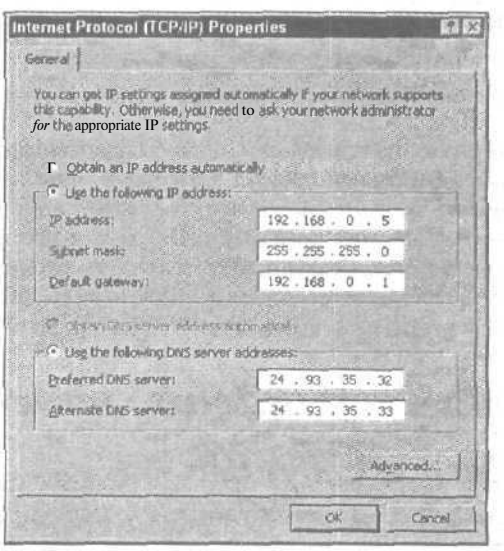


Рис. 14.1. Диалоговое окно Internet Protocol (TCP/IP) Properties

3. **Установите переключатель Internet Protocol (TCP/IP) и щелкните на кнопке OK.**
4. **Получив приглашение, введите путь к дистрибутивному компакт-диску.**
5. **Укажите детали конфигурации (об этом речь пойдет чуть позже).**

В диалоговом окне Internet Protocol (TCP/IP) Properties находятся поля для определения трех основных элементов конфигурации протокола IP. Обратите внимание на вариант выбора переключателя для автоматического получения IP-адреса. Этот параметр настраивает систему на запрос конфигурации IP у сервера DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации узла). Поскольку большинство серверов работает недостаточно хорошо при использовании динамических IP-адресов, вам может потребоваться определить статический IP-адрес для сервера Windows Server 2003 вместо использования службы DHCP. Вы должны либо получить общедоступный IP-адрес от вашего поставщика услуг Internet, либо использовать частный IP-адрес из одного из зарезервированных диапазонов адресов, определенных в RFC 1918.

Вы также должны вычислить маску подсети для вашей сети (в том случае, если вы не используете DHCP). Вы должны получить ее от поставщика услуг Internet, если вы используете общедоступный IP-адрес, либо можете вычислить свою собственную, если используете частные IP-адреса. В большинстве случаев при использовании частных IP-адресов маска подсети по умолчанию для класса адреса должна работать без преобразования или дополнительных вычислений.

Наконец, вы должны предоставить адрес шлюза по умолчанию для вашего сервера (до тех пор, пока вы не намерены использовать систему для взаимодействия с другими хост-узлами за пределами ее подсети). Шлюз по умолчанию должен быть адресом маршрутизатора в локальной подсети, к которой подключен сервер, способный перенаправить исходящий трафик в другие сегменты сети. В сетях, использующих общедоступные IP-адреса, это, возможно, будет маршрутизатор, брандмауэр или proxy-сервер, который соединяет локальную подсеть с другими подсетями и с Internet. В сетях, использующих частные IP-адреса, это, как правило, машина, на которой установлены proxy-сервер и программное обеспечение NAT и которая является посредником между локальной подсетью и Internet-соединением.

Диалоговое окно Internet Protocol (TCP/IP) Properties также содержит поля для настройки службы имен доменов — DNS. По большей части вы можете пропустить эти параметры... по меньшей мере, сейчас. Более подробно мы рассмотрим службу DNS в разделе "Трюки DNS".

После того как вы определите IP-адрес, маску подсети и шлюз по умолчанию, щелкните на кнопке OK, а затем закройте открытое вами окно и перезагрузите систему. Пока это все, что необходимо для настройки базовой конфигурации протокола TCP/IP для Windows 2003.

Более сложная настройка конфигурации необходима в том случае, если ваша сеть имеет большие размеры и, следовательно, сложнее. Чтобы справиться с этой сложностью, необходимо выполнить несколько большую работу. Щелкните на кнопке Advanced (Дополнительно) в диалоговом окне Internet Protocol (TCP/IP) Properties, чтобы открыть диалоговое окно Advanced TCP/IP Settings (Дополнительные параметры TCP/IP) с четырьмя вкладками. Ниже приведено краткое описание этих вкладок.

- ✓ IP Settings. Эта вкладка позволяет определить несколько сочетаний IP-адресов и масок подсетей для одного сетевого адаптера. Вы можете также определить дополнительные шлюзы по умолчанию, равно как и метрику интерфейса, которая используется маршрутизаторами (или службой маршрутизации в Windows 2003) для определения адреса, по которому следует отправлять данные, — путь с самым низким значением метрики используется первым.
- ✓ DNS. Эта вкладка позволяет определить дополнительные DNS-серверы — парочка, которую вы ранее определили в диалоговом окне Internet Protocol (TCP/IP)

Properties, также здесь присутствуют, так что не смущайтесь. Кроме того, вы можете задать способ поиска или разрешения вопросов на основе DNS-сервера, DNS-домена и дочерних DNS-доменов. Два переключателя в нижней части вкладки DNS позволяют воспользоваться динамической регистрацией для автоматического добавления IP-адреса вашего сервера и имени домена в локальную службу DNS. Подробно служба DNS описывается ниже, в разделе "Трюки DNS".

- **WINS.** На этой вкладке определяется IP-адрес для WINS-сервера (Windows Internet Name Service — служба имен Internet для Windows). WINS-серверы преобразуют NetBIOS-имена в IP-адреса. Служба WINS удобна для сетей Windows 2003 с несколькими серверами и сегментами. Эта вкладка также дает вам возможность контроля за тем, каким образом работает (и работает ли) интерфейс NetBIOS поверх протокола TCP/IP. Более подробно о WINS-службе можно узнать в разделе "WINS — выигрывают все!".
- Options. Используя эту вкладку, вы можете определить альтернативные параметры, связанные с TCP/IP. Эта вкладка представляет доступ исключительно к фильтрам TCP/IP по умолчанию, однако схема интерфейса наталкивает на мысль, что здесь можно настроить конфигурацию других дополнительных возможностей или служб, если их установить позже. Фильтры TCP/IP позволяют определить TCP, UDP (User Data Protocol — пользовательский протокол данных) и допустимые для использования порты протокола. Другими словами, они блокируют весь трафик за исключением трафика для портов, которые вы выбрали в качестве разрешенных. Этот интерфейс весьма ограничен, поскольку не сообщает, какие порты необходимо разблокировать. Для выполнения фильтрации мы рекомендуем развернуть proxy-сервер или брандмауэр, поскольку эти устройства обладают более дружественным интерфейсом и подсказывают, какие порты вам необходимы.

WINS — выигрывают все!

В сети Microsoft Windows хост-узлам TCP/IP можно давать NetBIOS-имена вместо IP-адресов или имен доменов. Поскольку NetBIOS-имена более-менее уникальны для сети Microsoft Windows, не существует действующих стандартов для связывания NetBIOS-имен с IP-адресами. В сети Microsoft Windows, которая использует протокол TCPJIP в качестве единственного сетевого протокола, важно иметь возможность разрешать NetBIOS-имена в IP-адреса. И здесь вступает в игру WINS (Windows Internet Name Service — служба имен Internet для Windows).

Беглый взгляд на WINS

Поскольку разрешение NetBIOS-имен в IP-адреса имеет решающее значение для обеспечения доступа ко многим встроенным службам и функциям Windows 2003, компания Microsoft предоставляет два метода управления этим процессом.

- **LMHOSTS.** Вы можете воспользоваться файлом LMHOSTS, чтобы создать статическую таблицу, которая связывает определенное NetBIOS-имя с определенным IP-адресом. (LM означает LAN Manager и указывает на сетевую операционную систему, которая предшествовала Windows NT.) Подобный файл должен присутствовать на каждой машине, чтобы обеспечить необходимые возможности преобразования имен в адреса.

  Для небольших простых сетей использование файла LMHOSTS — вполне приемлемый метод. Что касается больших и сложных сетей, значительный объем работы, необходимой для сопровождения большого количества подобных файлов, весьма быстро может выйти из под контроля.

- **WINS.** Эта служба вступает в игру в крупных, более сложных сетях. WINS функционирует на машинах под управлением Windows Server 2003 в качестве службы, которая автоматически обнаруживает NetBIOS-имена и управляет динамической базой данных, которая связывает NetBIOS-имена с IP-адресами. По мере роста сети иногда необходимыми становятся несколько служб WINS, чтобы способствовать более быстрой обработке запросов на разрешение имен.

  Один WINS-сервер может справиться со всей сетью. Однако в сетях, содержащих множество узлов и тысячи пользователей, несколько WINS-серверов могут распределить нагрузку, связанную с разрешением имен и тем самым ускорить доступ пользователей к ресурсам NetBIOS.

WINS-серверы обладают несколькими преимуществами по сравнению с LMHOSTS-файлами. Они создают динамическую базу данных, а это означает, что по мере изменения, появления новых и удаления прежних имен и адресов в сети база данных изменяется, как только WINS-сервер обнаруживает новую связь между именем и адресом либо старые имена с новыми адресами. WINS-серверы могут быть особенно важны для сетей, где используется служба DHCP, если клиенты также совместно используют файлы и принтеры на ее машинах. WINS-серверы в чем-то напоминают словарь, который постоянно обновляется по мере добавления новых слов (в нашем случае — имен).

WINS-серверы

WINS-серверы поддерживают базу данных, которая отображает имена компьютеров в соответствующие им IP-адреса и наоборот. Вместо того чтобы отправлять циркулярные сообщения с информацией об адресе, которые пожирают пропускную способность сети, рабочая станция, которой требуется разрешить NetBIOS-имя, осуществляет запрос непосредственно предназначенному для этого WINS-серверу (этой цели фактически служит вкладка WINS диалогового окна Advanced TCP/IP Settings).

Такой подход позволяет рабочей станции воспользоваться преимуществами определенной службы и быстро и эффективно получить информацию об адресе. Когда рабочие станции с NetBIOS-именами входят в сеть, они предоставляют информацию о себе и своих ресурсах WINS-серверу. Затем любые изменения автоматически отображаются в базе данных WINS-сервера.

Хотя служба WINS намного проще службы DNS, работать с ней не так легко. Вам необходимо установить WINS как компонент сетевой службы посредством интерфейса Network and Dial-up Connections (Сеть и удаленный доступ к сети). Но прежде чем приступить к этому процессу, ознакомьтесь с руководством, которое входит в состав пакета Resource Kit Windows 2003.

WINS-клиенты

При настройке конфигурации рабочих станций или серверов (по меньшей мере, тех серверов, которые не играют роль хост-узла для программного обеспечения WINS-сервера) сети вы предоставляете IP-адрес в распоряжение одного или нескольких WINS-серверов вашей сети. При загрузке эти машины сообщают WINS-серверу имя компьютера, имена сетевых ресурсов и IP-адрес. WINS-сервер работает иначе. Когда рабочей станции требуется IP-адрес, соответствующий NetBIOS-имени, она просит WINS-сервер предоставить ей эту информацию.

NetBIOS поверх TCP/IP

NetBIOS поверх TCP/IP — головная боль многих консультантов по системам безопасности — представляет собой комбинированный интерфейс прикладного программирования (Application Programming Interface — API), применяемый системой Windows 2003 для всех ее

внутренних и внешних (сервер–сервер) взаимодействий. В защищенной среде, например под защитой брандмауэра или proxy-сервера, использование NetBIOS поверх TCP/IP выгодно, поскольку обеспечивает поддержку многих дружественных по отношению к пользователю функциональных возможностей сетей Windows 2003. Но без соответствующей защиты — это зияющая брешь, которую могут использовать злоумышленники, чтобы завладеть вашей сетью или автономной системой. Вкладка WINS позволяет отключить использование NetBIOS поверх TCP/IP в действующей системе (подразумевается, что NetBIOS не будет передаваться по сетевым каналам с данного компьютера) или же разрешить ей выдать себя за DHCP-сервер (если DHCP-сервер запретил использование NetBIOS, эта система также подходит). Запрещение использования NetBIOS поверх TCP/IP стоит рассматривать только в том случае, если все системы в рамках сети представляют собой такие ОС, как Windows 2000/XP/2003, и ни одно приложение или служба в сети не требует функционирования NetBIOS. Другими словами, вам придется потерпеть NetBIOS еще какое-то время.

Трюки DNS

Один из способов упростить идентификацию хост-узлов TCPЯP состоит в использовании вместо IP-адресов FQDN (Fully Qualified Domain Name — полностью определенное имя домена). *FQDN* используется в качестве имени при идентификации ресурсов и позволяет облегчить доступ пользователю к этим ресурсам (например, `www.microsoft.com`). Преобразование имен доменов и FQDN-имен в IP-адреса — это ключевой вид сетевых услуг в общем и для Internet в частности, где используются сотни миллионов имен и адресов. Именно здесь вступает в силу служба имен доменов — Domain Name Service, называемая также службой именования доменов (Domain Naming Service) и системой имен доменов (Domain Naming System), но всегда известная под аббревиатурой DNS.

Так же как и для NetBIOS-имен и IP-адресов, связь между FQDN-именами и IP-адресами можно поддерживать двумя способами.

- ✓ Файл **HOSTS.** Вы можете создать в каждой системе файл HOSTS. Файл HOSTS поддерживает локальную таблицу, которая связывает определенные FQDN-имена с определенными IP-адресами. При изменении такой связи файл HOSTS необходимо обновить вручную и скопировать на все машины сети.

  HOSTS-файлы не предназначены для взаимодействия с большими IP-сетями, особенно с Internet. Это объясняет, почему HOSTS-файлы в большинстве случаев представляют собой пережитки прежней, более простой эпохи IP-сетей. Никто больше не использует HOSTS-файлы, разве что в качестве резервной системы на случай отказа службы DNS.
- ✓ DNS. Доступ к серверу DNS позволяет сетевым машинам запрашивать услуги по разрешению имен у этого сервера, а не поддерживать связи между именами и адресами самостоятельно. Хотя настройка конфигурации DNS-серверов должна осуществляться вручную, DNS-сервер может с легкостью справиться с потребностью разрешения имен для всей сети. DNS-серверы могут также взаимодействовать друг с другом, так что запрос на разрешение имени, который не может обработать локальный сервер, может передаваться вверх по иерархии FQDN-имен до тех пор, пока он не достигнет сервера, способного транслировать имя в адрес или указать на то, что данное имя неверно.

Internet содержит десятки тысяч DNS-серверов. Многими из этих серверов управляют поставщики услуг Internet; другие находятся под контролем специальных высокоуровневых уполномоченных доменов. Чтобы отметить границу присутствия Internet, вы должны получить уникальное FQDN-имя через InterNIC (или позволить сделать это за вас ISP). После получения этого имени оно связывается со специальным корневым IP-адресом в некотором DNS-сервере (вероятно, это сервер вашего ISP, если только вы не установите свой собственный DNS-сервер).

Когда стоит использовать DNS

Если только вы не располагаете крупномасштабной сложной сетью, то, вероятно, работаете с DNS-сервером, принадлежащим кому-то другому — скорее йсего, вашему ISP. Однако если вы имеете большую сеть, в которую входит более 1000 компьютеров, или же ваша сеть охватывает многочисленные узлы с помощью частных глобальных каналов, DNS-сервер поможет вам верно обозначить границы присутствия Internet.

Одна из уникальных особенностей системы Windows 2003 заключается в том, что она автоматически устанавливает на первом сервере домена три службы: Active Directory, DHCP и DNS. Хотя в действительности вам не обязательно применять службы DHCP и DNS, они все равно устанавливаются по умолчанию. Таким образом, установка этих служб — сущий пустяк (особенно, если учесть, что мастер настройки конфигурации вашего сервера — Configure Your Server Wizard — выполняет это автоматически). Серьезные проблемы могут возникнуть при попытке настроить конфигурацию DNS (или DHCP).

Где узнать больше о DNS

Если вас заинтересовала установка DNS-сервера, обратитесь к таким источникам технической информации, как Resource Kit Windows Server 2003 или TechNet. Мы также рекомендуем вам книгу *Служба DNS в Windows 2000,* как безупречное руководство по использованию Windows 2000 в качестве DNS-сервера. Хотя в названии присутствует Windows 2000, эта книга отлично подходит и для Windows 2003, поскольку DNS-служба осталась точно такой же.

DHCP: автоматизация IP-адресации

DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации узлов) используется для динамического присваивания системам IP-адресов и других параметров конфигурации при их загрузке. Это позволяет настроить конфигурацию клиента автоматически при запуске, что уменьшает усилия по их администрированию. Служба DHCP также позволяет большим группам клиентов совместно использовать небольшой пул IP-адресов, только если подключение к Internet в течение заданного времени необходимо лишь части этих клиентов.

Что такое DHCP

Служба DHCP также относится к службам, которые может автоматически предоставить Windows Server 2003. Другими словами, система Windows Server 2003 может запустить ПО DHCP-сервера для управления IP-адресами и предоставления информации о конфигурации практически для любого типа клиента TCP/IP.

Служба DHCP управляет распределением IP-адресов, арендуя их. Когда новая система, настроенная на использование службы DHCP, подключается к сети и требует данные о конфигурации, для этой системы арендуется IP-адрес (срок каждой аренды по умолчанию равен

трем дням). Когда половина срока аренды истекает, клиент может попросить возобновить ее на следующие три дня. Если этот запрос отклоняется или остается без ответа, запрос на возобновление аренды повторяется по истечении 87,5 и 100% времени аренды. Если срок аренды закончился и не возобновлен, клиент не может получить доступ к сети до тех пор, пока не получит в пользование новый IP-адрес. Инициировать возобновление или передачу в аренду IP-адреса можно вручную, указав в приглашении для ввода Windows 2003 команду `ipconfig/renew` или `ipconfig/release`.

Просмотреть текущее состояние конфигурации IP можно с помощью команды ipconfig. Введя в приглашение командной строки команду `ipconfig/all |more`, можно отобразить всю информацию, касающуюся конфигурации IP для машины, экран за экраном.

Встретится ли вам DHCP в будущем

По нашему мнению, существуют две причины, по которым службу DHCP можно рассматривать как большую удачу для администраторов Windows Server 2003, которым необходимо использовать ее.

- ✓ DHCP позволяет управлять всей совокупностью IP-адресов в одном месте, с одного сервера, прилагая лишь небольшие усилия сверх настройки начальной конфигурации адресного пула (диапазона адресов, к которому обращается DHCP в процессе управления). В прежние времена (до появления DHCP) управление IP-адресами обычно требовало значительно более частого похода от машины к машине.
- ✓ DHCP автоматически предоставляет IP-адреса и информацию о конфигурации (включая маску подсети и адреса шлюза по умолчанию) конечным пользователям машин. Благодаря этому при установке IP-клиентов и возникновении необходимости в управлении происшедшими изменениями конфигурации их осуществление не составляет никакого труда.

  Для настройки IP-конфигурации на новом клиенте все, что необходимо сделать конечным пользователям (или вам) в системах Windows 2003/NT/9x, — это щелкнуть на единственном переключателе в диалоговом окне Internet Protocol (TCP/IP) Properties, который называется Obtain an IP Address Automatically (Получить IP-адрес автоматически). Остальное сделает DHCP!

  Когда происходят изменения в конфигурации, они автоматически вносятся при возобновлении аренды IP-адресов. Вы можете даже отменить все существующие договоры аренды и заставить клиентов возобновить их договоры аренды всякий раз, когда значительная перенумерация или изменения конфигурации требуют немедленного обновления их IP-конфигурации.

Главная причина использования службы DHCP состоит в том, что она намного облегчает вашу работу. Применение DHCP рекомендуется для всех сетей, которые используют протокол TCP/IP для десяти и более клиентов. На первом сервере Windows Server 2003 домена служба DHCP устанавливается автоматически, но вам все же необходимо включить его и надлежащим образом настроить его конфигурацию, прежде чем он станет полезным для вас. Поэтому, если вы полагаете, что вас может заинтересовать установка DHCP-сервера, обратитесь к техническим руководствам, таким как Resource Kit для Windows Server 2003 или TechNet, чтобы изучить детали установки и настройки конфигурации.

Книги о TCP/IP

Если эта глава пробудила ваш интерес к TCP/IP, вы можете почерпнуть более подробную информацию из следующих отличных источников.

- ✓ Сети *TCP/IP, в* 3-х *томах.* Дуглас Камер.
- ✓ *TCP/IP* для *"чайников".* Кэндайс Лайден, **Маршалл** Виленски.

Выявление и устранение проблем

Проблемы, которые возникают в сетях TCP/IP, почти всегда связаны с неправильной настройкой конфигурации. Неверные IP-адреса, маски подсетей, шлюзы по умолчанию, DNS-, WINS- и DHCP-серверы могут поставить всю сеть, если не всю систему, на колени. Поэтому будьте чрезвычайно внимательны и дважды проверяйте все параметры и вносимые изменения, прежде чем ввести их в действие.

Если вы пользуетесь услугами поставщика услуг Internet, вы должны как можно раньше получить консультацию его персонала технической поддержки, чтобы, насколько возможно, избежать пробуксовки в использовании TCP/IP. Вы можете обнаружить, что источник проблем кроется не на вашей стороне, а на стороне поставщика услуг. В этом случае единственное, что вам остается, — проявить терпение, а затем пожаловаться. Если проблемы возникают слишком часто и вызывают у вас серьезное беспокойство, смените поставщика услуг Internet.

Windows Server 2003 включает немало средств, с помощью которых вы можете выявить источники проблем. Мы уже упоминали программу ipconfig; ниже приводится перечень некоторых других средств. Средства сетевой диагностики

- ✓ PING. Предназначено для проверки пути, по которому ваша система взаимодействует с другой удаленной системой. Если программа PING регистрирует отклик на посланный запрос, вы можете быть уверены, что связь прослеживается и удаленная система подключена к сети. Если программа PING не регистрирует отклика, это значит, что либо канал связи неработоспособен, либо удаленная система отключена от сети.
- ✓ TRACERT. Обнаруживает ретрансляции (с которыми сталкиваются системы) между вашей системой и удаленными системами. В результате вы получаете информацию о том, проходят ли ваши пакеты маршрутизации трассы и какая из систем отказала.
- ✓ ROUTE. Используется для просмотра и модификации таблицы маршрутизации многоканальных систем.
- ✓ NETSTAT. Отображает информацию о состоянии текущего соединения TCP/IP.
- ✓ NSLOOKUP. Отображает информацию о DNS, которая поможет вам управлять DNS-сервером и устранять проблемы.
- ✓ TELNET. Используется для установления текстового терминала, эмулирующего работу с удаленной системой. Программа Telnet обеспечивает доступ к удаленной системе таким образом, будто вы работаете на ее клавиатуре. Windows Server 2003 не включает входящего сервера Telnet.

Подробная информация, **касающаяся этих** средств, **включена в справочные файлы Windows** 2003, Windows Server **2003 Resource Kit** и TechNet.

Часть IV

Сеть в работе

"Централизованная система управления безопасностью звучит заманчиво, но что нам тогда делать с собаками?"

В этой части...

Итак, сервер Windows Server 2003 установлен и работает, но тут-то я" начинается самое интересное — сопровождение сервера и сети, которую вы с таким трудом создали. По крайней мере так думают многие. Поэтому, в полном смысле слова, часть IV начинается с того, чем закончилась часть III.

Сначала мы начнем с управления пользователями (и их группами), которые работают в вашей сети и используют ваш сервер. Затем мы перейдем к важнейшему обсуждению того, как установить разрешения файловой системы NTFS и совместно используемых ресурсов. После того как у вас появились данные и пользователи, нуждающиеся в защите, резервное копирование вашей системы больше не возможность — это абсолютная необходимость, вот почему эта тема стала на повестке дня управления системой. В завершение части IV вы узнаете о безопасности компьютеров и сетей.

Таким образом, часть IV охватывает все важнейшие темы, связанные с управлением сетями Windows Server 2003, и подготовит вас к самостоятельной работе с одной из таких сетей. Внимательно прочтите эти главы, и тогда ваши пользователи будут благодарить вас, а вы сэкономите время и силы.

Помните вот о чем: время а стоимость сопровождения занимают 90 процентов жизненного цикла компьютерной системы. Поэтому внедрение надежной процедуры сопровождения и четкое ее соблюдение являются ключевым фактором успешной работы сети. Воспользуйтесь благоприятной возможностью и не идите более тяжким путем познания...

Глава 15

Управление пользователями с помощью Active Directory

В этой главе...

- Определение свойств учетной записи пользователя
- Создание новых учетных записей пользователей и групп
- Управление учетными записями пользователей
- Знакомство с группами
- Присваивание профилей
- Управление операциями с помощью политик
- Устранение проблем

Учетные записи пользователей — обязательный элемент среды Windows Server 2003. Они — центральное средство управления и контроля, используемое операционной системой для идентификации пользователей, обеспечения доступа и проведения в жизнь контроля за ресурсами в локальной системе (и в рамках домена, и в рамках леса). Если вы не обладаете учетной записью пользователя в автономной системе Windows Server 2003 или в домене Windows Server 2003, вы не сможете получить доступ к этой системе или к ресурсам леса доменов. В этой главе рассматривается управление учетными записями пользователей и политиками домена с помощью консоли Active Directory Users and Computers.

Свойства учетных записей пользователей

Компьютеры обычно используются более чем одним человеком. Даже системы, которые работники используют исключительно на своих рабочих столах, допускают локальный вход для системных администраторов. Если эти системы обладают учетными записями компьютеров в рамках домена, для остальных пользователей существует возможность войти в эти системы с доменными учетными записями. Компьютеры различаются в зависимости от того, работает ли на них тот или иной человек, с помощью применения механизма безопасности, называемого *объектом учетной записи пользователя (user account object)*. Каждый пользователь, работающий на компьютере или в сети, обладает уникальной учетной записью пользователя, которая содержит детали, касающиеся пользователя, такие как его права и ограничения на доступ к ресурсам и др.

Учетная запись пользователя домена Windows Server 2003, связана или ассоциируется со следующими элементами.

1 ✓ Парольная защита. Учетная запись пользователя защищена паролем, поэтому только уполномоченное лицо может получить доступ к системе.

- ✓ Разрешения. Разрешения — это полномочия доступа, предоставляемые учетной записи пользователя. При этом учитываются членство в группах и специальные пользовательские параметры доступа к ресурсам.
- ✓ **Идентификация.** Учетная запись пользователя идентифицирует лицо для компьютерной системы и сети.
- ✓ Правя **пользователя.** Это высокоуровневые полномочия, которые могут быть предоставлены пользователю или группе для определения или ограничения их действий в этой компьютерной системе.
- ✓ **Роуминг.** Вы можете определить учетную запись пользователя так, что пользователь сможет войти в любую систему, которая является членом домена, с помощью учетной записи пользователя домена (некоторые пользователи могут зарегистрироваться с локальной учетной записью в определенной ситуации), службы удаленного доступа (Remote Access Service — RAS) или через шлюз.
- ✓ Схема среды. Профили являются специфическими для пользователя и хранят информацию о схеме, рабочем столе и среде пользователя в общем, только если они не ограничены специально посредством использования обязательных профилей. Вы можете определить профили так, что они будут сопровождать учетную запись пользователя независимо от того, в каком месте сети пользователь получает доступ.
- ✓ Аудит. Windows Server 2003 может отслеживать доступ и использование системы по учетным записям пользователей, если этот уровень аудита разрешен в домене.

Доступ к серверу Windows Server 2003 требует, чтобы пользователи успешно идентифицировали себя с помощью учетной записи пользователя домена. Это означает, что когда пользователь с надлежащим уровнем разрешения (не все обладают разрешением локально входить во все системы домена) садится за систему Windows Server 2003, он может войти на локальную машину с локальной учетной записью (это называется *интерактивным входом в систему (interactive logon)*). В этом случае, чтобы начать процесс регистрации, пользователь должен нажать комбинацию клавиш <Ctrl+Alt+Del>, а затем предоставить системе правильное имя пользователя и пароль. Аналогичным образом он может войти в систему с доменной учетной записью, если сервер является членом домена. После того как система проверит эту информацию, пользователю разрешается доступ. После завершения сеанса работы с системой пользователь может выйти из системы, которая становится доступной для входа следующего пользователя.

При установке Windows Server 2003 по умолчанию для автономной (не члена домена) системы автоматически создаются три учетные записи. Одна из них, учетная запись Administrator (Администратор), используется для начальной настройки конфигурации системы и создания других учетных записей пользователей. Вторая учетная запись, Guest (Гость), представляет собой быстрый способ организации низкоуровневого доступа для любого пользователя. Третья учетная запись пользователя, HelpAssistant (Помощник) (зачастую называемая Support_*<произвольныесимволы>*), служит в качестве основной учетной записи для сеансов удаленного доступа. Служба Remote Desktop Help Session Manager (Менеджер сеанса удаленной оперативной помощи) управляет учетной записью HelpAssistant, которая по умолчанию заблокирована.

Правь, администратор!

Учетная запись Administrator — основное средство, с помощью которого вы настраиваете конфигурацию Windows Server 2003- Это также наиболее мощная учетная запись в системе Windows Server 2003; поэтому вы должны быть уверены в том, что пароль для учетной записи Administrator сложный и секретный. Учетная запись Administrator обладает практически неограниченными возможностями управления доступом ко всем ресурсам Windows

Server 2003 (исключение составляет несколько системных процессов, которыми учетная запись Administrator не владеет и поэтому не имеет к ним доступа). Примерами являются управление пользовательскими учетными записями, манипулирование совместно используемыми ресурсами и предоставление полномочий доступа.

Учетная запись Administrator может "похвалиться" следующими свойствами.

- ✓ Вы не можете удалить ее.
- ✓ Вы не можете заблокировать или отключить ее.
- ✓ Вы можете (и должны) переименовать ее (щелкните правой кнопкой мыши на учетной записи и выберите пункт меню Rename (Переименовать)).
- ✓ Хотя определение пустого пароля для локальной учетной записи Administrator и допускается, однако это крайне нежелательно и считается скверной практикой безопасности. В определенных ситуациях некоторые службы не могут нормально работать, если вы не предоставите пароль. Поэтому вы должны обеспечить для этой учетной записи верно выбранный сложный пароль.

Переименование этой учетной записи считается хорошей практикой безопасности. Потенциальным хакерам (т.е. людям, которые стремятся получить несанкционированный доступ к вашей системе) необходимы всего два элемента информации, чтобы получить доступ к вашей системе: имя учетной записи и пароль. До тех пор, пока вы не переименовали эту учетную запись, они уже обладают половиной информации, необходимой, чтобы получить доступ к самой мощной учетной записи в вашей системе. А если вы к тому же не защитили свою учетную запись паролем, то это — единственное, что им требуется.

Гости могут и надоесть

Учетная запись Guest — вторая учетная запись, создаваемая по умолчанию системой Windows Server 2003. Вы можете использовать эту учетную запись как временный метод организации общего доступа. Она обладает минимумом прав доступа и ограниченными полномочиями на ресурсы.

Учетная запись Guest обладает следующими свойствами.

- ✓ Вы не можете удалить ее.
- ✓ Вы не можете заблокировать или отключить ее (она отключена по умолчанию).
- ✓ Вы можете переименовать ее.
- ✓ Она может обладать пустым паролем (она обладает им по умолчанию).
- ✓ Изменения среды не сохраняются этой учетной записью (т.е. профиль пользователя обязателен, поскольку пользовательские изменения в среде не сохраняются).

Учетная запись Guest может быть брешью в системе безопасности. Надежная практика безопасности рекомендует, чтобы вы держали эту учетную запись отключенной, переименовали ее и присвоили надлежащий пароль.

Создание учетных записей Active Directory

Создание учетных записей Active Directory для пользователей, входящих в домен и лес с целью доступа к ресурсам, — обычная и простая задача. Для создания и управления учетными записями пользователей и групп доменов в системе Windows Server 2003 используется

консоль Active Directory **Users** and Computers, окно которой показано на рис. 15.1. Создать пользовательскую учетную запись нетрудно, однако вам следует обратить внимание на множество деталей. Сначала мы опишем процедуру создания пользовательской учетной записи на скорую руку. Затем мы поговорим обо всех настройках, которые вы можете выполнить для этой учетной записи.

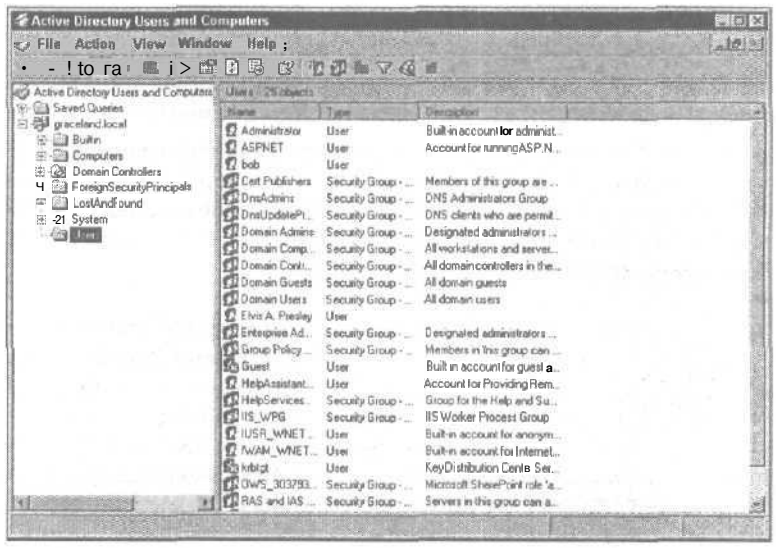


Рис. 15.1. Консоль Active Directory Users and Computers

1. **Чтобы открыть консоль Active Directory Users and Computers, выберите команду Start⇨All Programs⇨Administrative Tools⇨Active Directory Users and Computers (Пуск⇨Программы⇨Администрирование⇨Active Directory — Пользователи и компьютеры).**

2. **Дважды щелкните мышью на контейнере домена или производственного подразделения, которому вы хотите назначить учетную запись.**

   Вы видите на экране все используемые по умолчанию параметры для этого домена или производственного подразделения, включая учетные записи пользователей. Если вы назначаете учетную запись пользователя контейнеру Users (Пользователи) и щелкаете на ней, вы видите учетные записи Administrator и Guest, а также другие учетные записи, которые Windows Server 2003 устанавливает в зависимости от того, какие службы вы инсталлировали.

   Производственное подразделение (*organizational unit*) — это контейнер Active Directory, который включает другие производственные подразделения, компьютеры, учетные записи пользователей и группы. Более подробную информацию о производственных подразделениях см. в главе 11.

3. **Вы можете создать новую учетную запись пользователя с нуля, выделив для этого контейнер, в который вы намерены поместить ее, а затем выбрав на панели инструментов команду Action⇨New⇨User (Действие⇨Новый⇨Пользователь).**

   (Вы можете также щелкнуть правой кнопкой мыши на контейнере и выбрать команду New⇨User из раскрывающегося меню.) Откроется окно мастера New

Object — User (Новый объект — пользователь), показанное на рис. 15.2, Когда вы создаете пользовательский объект с нуля, вы должны обратить внимание на каждую деталь этой учетной записи.

4. **Введите следующую информацию,**

   - **First name (Имя); Last Name (Фамилия); Initial (Инициалы).** Введите имя пользователя, его фамилию и инициалы, если это необходимо.
   - **Full name (Полное имя).** В таком виде имя будет отображаться в системе. Заметьте, что мастер установки ввел имя за вас. Вы можете заменить введенное имя и выбрать подходящее отображение полного имени. Обычно отображается имя, а затем фамилия.
   - **User logon name (Имя пользователя для входа в систему).** Введите информацию, которую будет применять пользователь для того, чтобы подтвердить свою идентичность сети. Для этого типа имен вы должны создать фирменный стандарт, например фамилия и первый инициал, или нечто подобное. (Обратитесь к врезке "Что значит имя?", ниже в этой главе.)

     User logon name (Pre-Windows 2000) — имя пользователя для входа в систему, которое дается пользователю для систем, предшествующих Windows 2000. Обратите внимание, что мастер ввел эту информацию за вас. Вам нет необходимости изменять ее, если только вы не технический специалист.

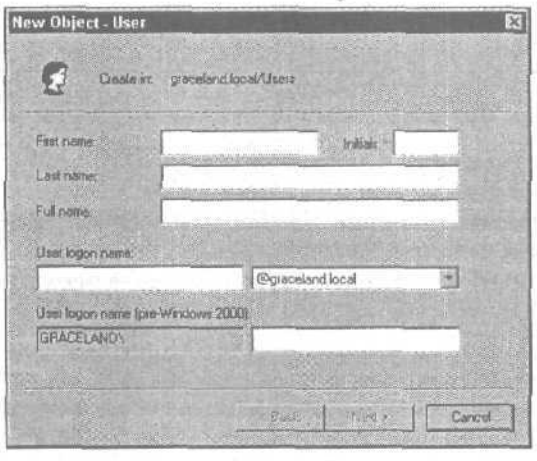


Рис. 15.2. Окно мастера New Object — User

5. **Чтобы продолжить установку этого нового объекта учетной записи пользователя, щелкните на кнопке Next (Далее).**

   В следующем окне введите информацию о пароле.

6. **Введите пароль для этой учетной записи, а затем подтвердите пароль для системы, введя его повторно.**
7. **Настройте параметры конфигурации пароля, используя опции, приведенные ниже.**

- **Флажок User Must Change Password at Next Logon (Потребовать смену пароля при следующем входе пользователя в систему).** Заставляет пользователя изменить пароль.
- **Флажок User Cannot Change Password (Запретить смену пароля пользователем).** Не позволяет пользователю изменить пароль.
- **Флажок Password Never Expires (Срок действия пароля не ограничен).** Освобождает эту учетную запись от правила, которое требует замены пароля по истечении заданного интервала времени.
- **Флажок Account is Disabled (Отключить учетную запись).** Гарантирует, что эту учетную запись нельзя использовать для получения доступа к системе. Вполне возможно, что при создании нового объекта-пользователя вы не будете выбирать эту опцию, поскольку захотите, чтобы пользователь имел возможность доступа к системе.

8. **Установив флажки, щелкните на кнопке Next.**

   Появится окно, которое позволит подтвердить выбранные вами варианты.

9. **Если все верно, щелкните на кнопке Finish (Готово). Если вы решили добавить другие параметры, щелкните на кнопке Back (Назад), чтобы сделать это немедленно. Если вам понадобится добавить данные позже, вы также сможете отредактировать свойства учетной записи.**

Что значит имя?

Windows Server 2003 в действительности не использует и даже не интересуется именем человека, присвоенным учетной записи. Для распознавания и отслеживания пользовательских учетных записей Windows Server 2003 использует идентификатор системы защиты (Security Identifier — SID). Но, поскольку вы человек, вы должны применять, где только возможно, имена, удобные для восприятия человеком. Это снимает напряжение и облегчает управление пользователями.

Мы ведем к тому, что вы должны применять соглашение об именовании — заранее определенный метод для создания имен пользователей, компьютеров, ресурсов и других объектов. Соглашению об именовании присущи два основных свойства: возможность всегда создавать новые (уникальные) имена и способность создаваемых имен нести описательную информацию об именуемом объекте.

Для небольших сетей редко требуется сложное или заранее определенное соглашение об именовании. Однако когда количество именованных элементов в сети достигает 100, вы можете обнаружить, что вам все труднее запоминать, кто такой или что такое на самом деле jackal, herbie и 8675309. Поэтому использование соглашения об именовании с начала развертывания небольшой сети может облегчить процесс ее наращивания в будущем.

Система Windows Server 2003 не предполагает использования какой-либо определенной схемы именования. Она оставляет вопрос определения имен на ваше усмотрение. Если вы решили использовать соглашение об именовании, вам необходимо проявить усердие при внедрении и применении этой схемы. Какое соглашение об именовании вы выберете или создадите, не имеет значения; главное, что оно всегда должно обеспечивать новые имена и эти имена должны нести информацию об объектах, которые они обозначают. Ниже приведены некоторые общие правила для соглашения об именовании.

- ✓ Имена должны быть согласованы для всех типов элементов (имен пользователей, имен компьютеров, имен сетевых ресурсов, имен каталогов и т.д.).
- ✓ Имена должны быть понятны (если они слишком сложны или трудны, их не станут использовать).
- ✓ Имена должны некоторым образом указывать на тип объекта.

г. Вы можете создавать новые имена, имитируя структуру существующих имен. Ниже приведены некоторые примеры частичного соглашения об именовании, которое вы можете использовать для своей сети.

- ✓ Имена пользователей можно создавать, комбинируя имя и фамилию пользователя (например, JohnSmith или Jsmith).
- ✓ Имена пользователей можно создавать, комбинируя фамилию пользователя и код подразделения (например, SmithAcct Smithsales5). При наличии Active Directory в этом виде разработки имен нет особой нужды, поскольку во многих случаях схема структуры вашего контейнера для производственного подразделения отражает сферы деятельности вашей компании.
- ✓ Имена компьютеров можно создавать, комбинируя имя пользователя с кодом типа компьютера или номером комнаты (например, SmithW98 или JS102).
- ✓ Имена групп можно создавать, комбинируя описание ресурса, местоположение, название проекта или подразделения (например, Tower12, Planning2 или Conferences12).
- ✓ Имена сетевых ресурсов или каталогов можно создавать, комбинируя дескриптор содержания или назначения с именем группы или проекта (например, Documents, SalesDocs или AcctSheet).
- ✓ Имена принтеров можно создавать, комбинируя тип модели, местоположение, наименование подразделения или группы (например, HP5Sales, CLJRm202 или HP4Acct).

Как вы видите, каждая из этих рекомендуемых частичных схем именования позволяет создавать новые имена и предоставляет достаточно информации об именуемом объекте, чтобы определить, где он расположен и является ли он учетной записью пользователя, компьютером, сетевым ресурсом или принтером.

Вы только что создали новый объект учетной записи пользователя домена и увидели этот объект в окне консоли Active Directory Users and Computers. На шаге 1 мы упомянули о способе отображения имени; именно с помощью этого способа вы должны просматривать список имен объектов.

Если вы щелкнете правой кнопкой мыши на новом объекте, а затем щелкнете на пункте меню Properties, то увидите несколько вкладок, включая вкладки General, Address, Account, Profile и др.

Вы можете использовать эти вкладки для ввода дополнительной информации о новом объекте учетной записи пользователя, такой как группа, к которой он принадлежит. Вы можете увидеть и другие вкладки, в зависимости от того, какие службы установлены в вашей системе Windows Server 2003 и является ли сервер автономным сервером, членом домена или контроллером домена.

В следующих разделах мы рассмотрим по отдельности некоторые используемые по умолчанию вкладки для сервера-члена домена, так что вы узнаете, как и что в них заполнять.

Вкладка General

Чтобы ввести дополнительную информацию об учетной записи, такую как описание (дополнительная информация о расположении, назначении учетной записи и другая информация по вашему усмотрению), адрес офиса, телефонный номер, адреса Web-страниц и адреса электронной почты, щелкните на вкладке General (Общие). Чем больше информации вы введете сейчас, тем больше она вас выручит впоследствии. Описательная информация отобразится в консоли Active Directory Users and Computers, если вы воспользуетесь детализированным представлением (View⇨Detail (Вид⇨Подробности)).

Вкладка Address

Щелкните на вкладке Address (Адрес), чтобы ввести информацию о физическом почтовом адресе пользователя. Хотя эта информация не требуется, ее полезно иметь под рукой.

Вкладка Account

Щелкните на вкладке Account (Учетная запись), чтобы получить доступ к имени пользователя для входа в систему, к имени пользователя для входа в системы, предшествующие Windows 2000, к информации о времени входа в систему, ограничениям рабочей станции (которые можно установить с помощью кнопки Log on) и информации о сроке действия учетной записи. Большая часть опций этой вкладки самоочевидны — за исключением информации о времени входа в систему и сроке действия учетной записи, которые описаны ниже.

- ✓ Время входа в систему. Щелкните на кнопке Logon Hours (Время), чтобы открыть диалоговое окно Logon Hours (рис. 15.3). В этом диалоговом окне вы можете определить время (в часах), в течение которого пользователь может получить доступ к системе. Если пользователь с этой учетной записью пытается войти в систему в неурочные часы, вход в систему не удастся. Если пользователь продолжает работать с системой, когда время его работы истекает, то он остается подключенным к системе, но не может установить ни одного нового сетевого соединения (т.е. не может отправить документ на принтер или открыть новый файл). Вы определяете время доступа с помощью выбора секций для дней недели и времени суток (в часах) и переключателя Logon Permitted (Вход в систему разрешен) или Logon Denied (Вход в систему запрещен). Этот переключатель в основном используется для тех, кто работает с системой по контракту; этим пользователям разрешено использовать систему только в течение обычного рабочего времени.
- ✓ Срок действия учетной записи. Установите переключатель Account Expires End Of (Срок действия учетной записи заканчивается), чтобы определить, когда заканчивается срок действия учетной записи (если это имеет место). Используется для пользователей, которые работают с системой на контрактной или временной основе, — доступ к системе им предоставляется только в определенное время.

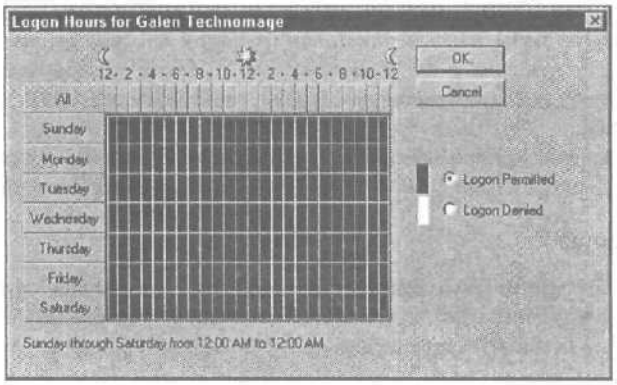


Рис. *15.3. Доступ* ***можно установить в*** *определенное время* ***и дни*** *недели*

Вкладка Profile

Щелкните на вкладке Profile (Профиль) диалогового окна Properties, чтобы отобразить текущую информацию о профиле учетной записи пользователя (рис. 15.4). В этом диалоговом окне вы можете задать следующую информацию.

- **Путь к профилю пользователя (Profile path).** Определение места, где хранится перемещаемый профиль для этого пользователя. Перемещаемый профиль позволяет пользователю получить доступ к своей рабочей среде с любой рабочей станции сети. (Более подробно об этом рассказывается ниже, в разделе "Снабдите своих пользователей подходящим профилем").
- **Имя сценария входа в систему (Logon Script).** Наименование файла для файла сценария, который должен выполняться при входе в систему. Обычно сценарий входа в систему — это пакетный файл, который определяет пути, устанавливает переменные среды, отображает диски и выполняет приложения. При работе с Windows Server 2003 обычно вы используете сценарии входа в систему для обеспечения совместимости с более старыми версиями серверов или DOS-приложениями либо для автоматической настройки конфигурации параметров доступа к серверу NetWare.
- **Домашний каталог (Home directory).** Используемое по умолчанию место хранения данного профиля, указываемое как локальный путь или буква диска, отображаемая на сетевом диске.

Вкладка Telephones

Щелкните на вкладке Telephones (Телефоны) диалогового окна Properties, чтобы ввести любой телефонный номер, по которому можно соединиться с человеком, такой как номер пейджера, факса или мобильного телефона. Во вкладке имеется даже раздел Comments (Комментарии), куда вы можете добавить любую информацию, которую сочтете необходимой.

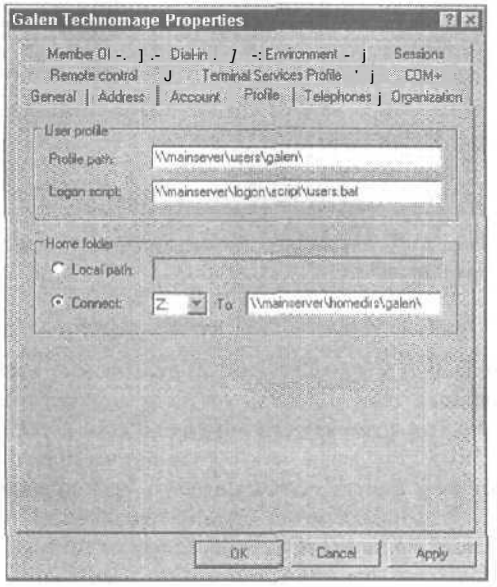


Рис. 15.4. Пример вкладки Profiles для пользователя

Вкладка Organization

Щелкните на вкладке Organization (Организация) диалогового окна Properties, чтобы ввести информацию о должности пользователя в организации и именах лиц, перед которыми он непосредственно отчитывается. Если ваша организация подвергается реорганизации, можете не заполнять вкладку.

Вкладка Member Of

После щелчка на вкладке Member Of (Член групп) диалогового окна Properties в ней отображается информация о состоянии учетной записи члена группы (рис. 15.5). В этой вкладке вы можете добавить объект учетной записи пользователя в группу или удалить объект учетной записи пользователя из группы. Если вы намерены добавить этот объект в другую группу, щелкните на кнопке Add (Добавить) и выберите группу. Как вы узнаете ниже, членство в группе определяет ресурсы, которым вы предоставляете доступ к учетной записи пользователя.

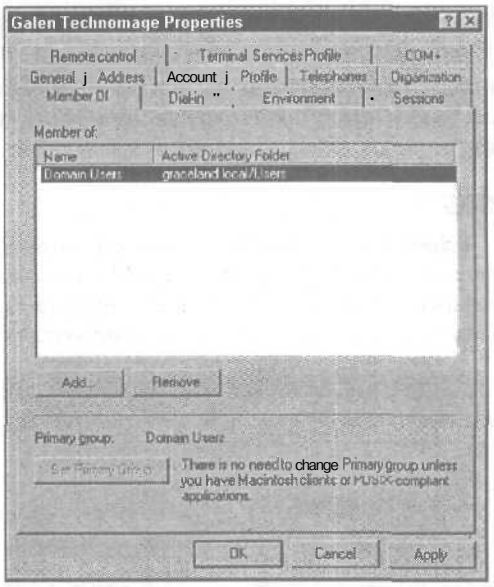


Рис. 15.5, Участие в группе определяется на этой вкладке

Вкладка Dial-in

Щелкните на вкладке Dial-in (Входящие звонки) диалогового окна Properties, чтобы разрешить или запретить пользователю с данной учетной записью входить в сеть. На этой же вкладке вы можете установить возможности обратного вызова. *Обратный вызов (callback)* означает, что при входе пользователей в сеть сервер осуществляет обратный вызов по предустановленному телефонному номеру, чтобы поверить, что пользователи действительно те, за кого они себя выдают. Этот номер может быть предустановлен или установлен пользователем. Обратный вызов часто используется для обеспечения безопасности, но он не особенно хорошо работает, когда пользователь находится в пути и останавливается в гостиницах, которые имеют разные телефонные номера. Эту возможность следует использовать с осторожностью.

Бесцеремонное обращение с пользователями

В некоторый момент вашей деятельности по управлению сетью вам может потребоваться отключить, переименовать или удалить учетные записи пользователей. Все эти функции можно выполнить с помощью консоли Active Directory Users and Computers.

Отключение (Disabling) учетной записи происходит тогда, когда вы блокируете учетную запись так, что ее нельзя использовать, чтобы войти в систему. Чтобы заблокировать учетную запись, выделите учетную запись пользователя, а затем выберите команду Action⇨Disable account (Действие⇨Отключить учетную запись). При создании объекта-пользователя с помощью мастера установки (см. выше раздел "Создание пользователей") вы можете установить флажок Account Is Disabled (Отключить учетную запись), и учетная запись пользователя будет отключена до тех пор, пока вы ее не разблокируете.

Переименование (Renaming) учетной записи пользователя изменяет имя учетной записи. Выберите учетную запись пользователя, а затем выполните команду Action⇨Rename (Действие⇨Переименовать). Диалоговое окно предлагает вам ввести новое имя. Обратите внимание, что изменение имени не изменяет идентификатор безопасности (SID) учетной записи.

Удаление (Delete) учетной записи пользователя удаляет учетную запись пользователя из системы. Выделите учетную запись пользователя, которую вы намерены удалить, а затем выберите команду Action ⇨ Delete (Действие⇨Удалить). Вы получите запрос на подтверждение удаления. При удалении учетной записи она выходит из употребления. SID-идентификатор удаленной учетной записи никогда не используется повторно. Создание новой учетной записи с такой же конфигурацией, как у удаленной учетной записи, по-прежнему приводит к созданию другой учетной записи, поскольку для нее используется новый SID-идентификатор; поэтому, поскольку речь идет о базе данных учетных записей, это новая учетная запись.

Когда пользователь покидает вашу организацию, вам необходимо решить, намерены ли вы оставить его старые учетные записи для использования его преемниками. Это наилучшее решение, поскольку оно позволяет сохранить все установки для подразделений и групп, однако это означает, что вы должны изменить всю личную информацию, чтобы она касалась новых пользователей.

Как на счет групп?

Группа — это совокупность пользователей, которым требуется сходный уровень доступа к ресурсам. Группы представляют собой основное средство, с помощью которого контроллер домена Windows Server 2003 предоставляет пользователю доступ к ресурсам.

Группы упрощают процесс администрирования за счет уменьшения количества взаимосвязей, которыми вам приходится управлять. Вместо того чтобы разбираться, каким образом каждый отдельный пользователь связан с каждым из ресурсов, вам требуется только управлять значительно меньшим количеством связей групп с ресурсами и знать, к какой группе принадлежит каждый из пользователей. Уменьшение нагрузки при этом составляет 40-90 процентов. В справочном руководстве по Windows Server 2003 имеется раздел Best Practices, посвященный лучшим методам организации управления, который призывает вас при любой возможности использовать группы.

Группа — это именованная совокупность пользователей. Существуют два различных типа групп, каждый из которых может обладать одной из трех областей действия.

- ✓ Группы безопасности (Security group). Используются для назначения пользователям прав на объекты и ресурсы в Active Directory. Вторичной функцией группы безопасности является то, что ее также можно использовать для посылки сообщений электронной почты всем членам группы.
- ✓ **Группы распространения (Distribution group).** Используются только для посылки сообщений электронной почты всем членам группы. Группы распространения нельзя использовать для определения разрешений на ресурсы и объекты в Active Directory.

Оба типа групп могут обладать следующими областями действия.

- ✓ Глобальные группы (Global Group). Существуют на уровне домена. Они присутствуют на каждом компьютере в пределах домена и управляются средствами консоли Active Directory Users and Computers с сервера Windows Server 2003. Если домен работает под управлением Windows 2000 в собственном режиме или в режиме Windows Server 2003, члены глобальных групп могут включать учетные записи и глобальные группы из этого же домена. Если домен работает под управлением Windows 2000 в смешанном режиме, члены глобальных групп могут включать учетные записи из этого же домена.
- ✓ **Локальные группы домена (Domain Local Group).** Существую только на одном компьютере. Они не представлены в рамках домена. Если домен работает под управлением Windows 2000 в собственном режиме или в режиме Windows Server 2003, члены локальной группы домена могут включать учетные записи, глобальные группы и универсальные группы из любого домена, а также локальные группы домена из этого же домена. Если домен работает под управлением Windows 2000 в смешанном режиме, члены локальной группы домена могут включать учетные записи и глобальные группы из любого домена.
- ✓ **Универсальные группы (Universal group).** Расширяют сферу влияния за пределы домена на все домены текущего леса. Если домен работает под управлением Windows 2000 в собственном режиме или в режиме Windows Server 2003, члены универсальной группы домена могут включать учетные записи, глобальные группы и универсальные группы из любого домена, а также локальные группы домена из этого же домена. Если домен работает под управлением Windows 2000 в смешанном режиме, возможно создание групп безопасности со сферой действия как у универсальных групп. Если домен работает под управлением Windows 2000 в собственном режиме или в режиме Windows Server 2003, возможно создание и использование универсальных групп для содержания других групп, таких как глобальные группы, чтобы облегчить назначение разрешений на ресурсы в любом домене лесе.

Три области действия групп упрощают взаимодействие пользователей с ресурсами. Использование групп значительно уменьшает нагрузку по администрированию для средних и больших сетей. Что касается небольших сетей, то оно может показаться несколько более сложным. Вы можете, например, использовать группы следующим образом.

- ✓ Локальным группам назначены уровни доступа к ресурсам.
- ✓ Для пользователей определена принадлежность к глобальной или универсальной группе.
- ✓ Глобальная или универсальная группа определена в качестве члена локальной группы.

Таким образом, пользователям предоставлен доступ к ресурсам за счет их принадлежности к локальной или универсальной группе. В свою очередь, принадлежность этих групп к локальной группе обеспечивает доступ к ресурсам.

Ниже приведены некоторые важные правила, касающиеся групп.

- ✓ Пользователь может быть членом нескольких глобальных или универсальных групп.
- ✓ Пользователи глобальной или универсальной группы могут быть членами нескольких локальных групп.
- ✓ Может существовать несколько локальных групп, которым разрешен доступ к некоторому ресурсу. Используя несколько локальных групп, можно назначить несколько уровней доступа к ресурсу: от операций чтения/печати до операций изменения/управления и вплоть до полного контроля.

Хотя учетные записи пользователя можно добавить непосредственно к универсальной группе, более эффективно добавлять их только к глобальным группам, а эти глобальные группы добавлять к универсальным группам. Когда принадлежность к универсальной группе изменяется, например за счет добавления или удаления учетных записей пользователей или групп, изменение должно тиражироваться в пределах леса посредством серверов глобального каталога (Global Catalog Services). Частое добавление или удаление учетных записей пользователей из универсальной группы может привести к серьезным проблемам, связанным с сетевым трафиком тиражирования изменений в пределах всего леса.

Если вы добавляете глобальную группу к универсальной, учетные записи пользователя и вложенные глобальные группы можно добавлять и удалять из глобальной группы, не вызывая при этом ни единой операции тиражирования. Подобный результат достигается благодаря тому, что принадлежность универсальной группы не изменяется! Она по-прежнему содержит в себе ту же глобальную группу или группы. Принадлежность глобальной группы изменяется только в том случае, когда вы добавляете или удаляете учетные записи пользователей или вложенные глобальные группы.

Хотя вы можете установить для пользователя прямую принадлежность локальной группе или даже прямой доступ к ресурсу, подобный подход разрушает ясную небольшую схему, которую компания Microsoft разработала, чтобы упростить вам жизнь. Так что просто следуйте этой рекомендации.

Несмотря на то что любая другая группа может быть членом локальной группы, последняя не может быть членом любой другой группы, если домен работает в смешанном режиме. Локальные группы домена можно поместить в другие локальные группы того же домена, если домен работает под управлением Windows Server 2000 в собственном режиме или в режиме Windows Server 2003.

Вы управляете группами в системах под управлением Windows Server 2003 с помощью консоли Active Directory Users and Computers. Чтобы создать группу с использованием консоли Active Directory Users and Computers, выполните следующие действия.

1. **Щелкните на контейнере домена, к которому вы намерены добавить группу, а затем выберите команду Action⇨New⇨Group (Действия⇨Новая⇨Группа).**

   Появится диалоговое окно New Object — Group (Новый объект — Группа).

2. **Введите имя новой группы.**

   Имя группы для машин, работающих под управлением ОС Windows — предшественников Windows Server 2003, заполняется автоматически.

3. **В диалоговом окне New Object — Group выберите область действия группы: локальная (Local), глобальная (Global) или универсальная (Universal) группа домена.**

   Универсальные группы — мощное средство, поскольку их область действия распространяется на все домены текущего леса.

4. **Выберите тип группы: группа безопасности (Security Group) или группа распространения (Distribution Group).**

   Вам почти никогда не придется использовать установку группы распространения, поскольку она не содержит информации ACL-списка, необходимой для целей безопасности. Установка группы распространения используется в основном для операций электронной почты, где вам может потребоваться отправить сообщения группе пользователей и где не требуется подключение безопасности. Мы рекомендуем всегда применять в качестве типа группы группу безопасности.

5. **Щелкните на кнопке OK.**

После того как объект группы создан, вы можете дважды щелкнуть на объекте группы, чтобы добавить к нему дополнительные атрибуты. Вы увидите несколько новых вкладок: General, Members, Member Of и Managed By.

- ✓ **General (Общие).** Содержит ту же информацию, которую вы заполняли при создании группы (имя группы, описание, адрес электронной почты, область действия группы и тип группы).
- ✓ **Members (Члены).** Содержит имена пользователей, которые являются членами группы. Именно на этой вкладке вы добавляете пользователей в группу.
- ✓ **Member Of (Член групп).** На этой вкладке можете добавить группу в другие группы.
- ✓ **Managed By** (Управляются с помощью). Эта вкладка позволяет определить, кто управляет группой. Вы можете задать информацию о пользователе, например имя, адрес и номер телефона.

Вам нет нужды создавать свои собственные группы: контроллеры домена Windows Server 2003 обладают несколькими встроенными локальными группами домена, которыми вы можете воспользоваться. По умолчанию группы расположены в контейнере Builtin (Встроенные). Приведенный список включает лишь некоторые из них (члены групп, используемые по умолчанию, заключены в скобки).

- ✓ Administrators (Administrator (Администратор), Domain Admin (Администратор домена), Enterprise Admin (Администратор предприятия).
- ✓ Guests (Domain Guests (Гости домена), Gusts (Гости)).
- ✓ Pre-Windows 2000 Compatible Access (Анонимный вход в систему, Everyone (Все)).
- ✓ Users (Domain Users (Пользователи домена), Authenticated Users (Санкционированные пользователи)).

Обратите внимание, что встроенные группы, отображаемые на вашем экране, могут содержать больше членов, чем в приведенном нами списке, в зависимости от установленных на вашем сервере служб. Например, если вы установили службу IIS (Internet Information Server — информационный сервер Internet), то увидите больше членов встроенной группы Guest.

Эти установленные по умолчанию локальные группы безопасности домена обладают как встроенными возможностями (см. рис. 15.6), так и правами пользователей по умолчанию. Вы можете модифицировать пользовательские права этих групп (см. раздел "Свойства учетных записей пользователей" в этой главе), однако вы не можете изменить возможности.

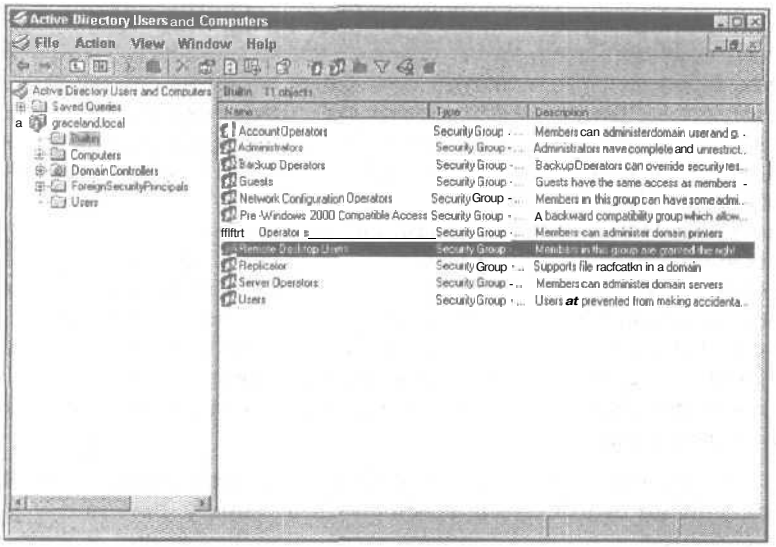


Рис. 15.6. Встроенные группы безопасности Windows Server 2003

Контроллеры домена Windows Server 2003 включают также следующие дополнительные группы безопасности, которые содержатся по умолчанию в контейнере Users.

- ✓ Cert Publishers (Сертифицированные авторы публикаций — локальная группа домена).
- ✓ Debugger Users (Пользователи отладчика — локальная группа домена).
- ✓ HelpServicesGroup (Группа справочной службы — локальная группа домена).
- ✓ RAS and IAS Servers (Локальная группа домена служб RAS и IAS).
- ✓ Telnet Clients (Клиенты Telnet — локальная группа домена).
- ✓ Domain Admins (Администраторы домена — глобальная группа).
- ✓ Domain Computers (Компьютеры домена — глобальная группа).
- ✓ Domain Controllers (Контроллеры домена — глобальная группа).
- ✓ Domain Guests (Гости домена — глобальная группа).
- ✓ Domain Users (Пользователи домена — глобальная группа).
- ✓ Group Policy Creator (Автор политики групп — глобальная группа).
- ✓ Enterprise Admins (Администраторы предприятия — универсальная группа).
- ✓ Schema Admins (Администраторы схемы — универсальная группа).

Могут существовать и другие группы, например DnsAdmins, которая создается, если контроллер домена управляет службой DNS. Однако в основном предыдущий список охватывает все группы для контроллера корневого домена леса.

Система Windows Server 2003 обладает еще тремя группами, которые она относит к особым сущностям: Everyone (Все), Network (Сеть) и Interactive (Интерактивная). Это встроенные группы, которые вы можете модифицировать только косвенно. Например, группа Everyone может отражать принадлежность 20 учетных записей пользователя до тех пор, пока вы не добавите еще одну учетную запись к домену. Пользователь добавляется в группу Everyone автоматически без всякого вмешательства с вашей стороны. Поэтому хотя вы специально не определяете принадлежность учетной записи группе Everyone, вы косвенно

влияете на эту принадлежность. Гостевые учетные записи также добавляются в группу Everyone, поэтому следует проявлять осторожность и модифицировать учетную запись Guest таким образом, чтобы ограничить доступ к сети. (Более подробно этот тип учетных записей описан выше, в разделе "Бесцеремонное обращение с пользователями".)

Группа Network предназначена для тех, кто использует сеть как средство доступа к ресурсам. Если вы предоставляете пользователям доступ к ресурсам всей сети, они автоматически добавляются к группе Network.

Еще одна группа, Interactive, представляет пользователей, которые обращаются к ресурсам посредством регистрации или локально.

Вы не можете изменить принадлежность к этой группе в прямом смысле. Однако когда вы устанавливаете разрешения на ресурсы, эти группы также оказываются в вашем распоряжении и вы должны модифицировать уровень доступа этих групп к определенным ресурсам. Например, при предоставлении пользователям доступа к корневому уровню тома вы можете ограничить доступ для группы Everyone так, что эти пользователи будут обладать разрешением только на операцию Read (Читать).

Вы должны создавать группы, которые соответствуют структуре вашей организации, методам ее работы или просто здравому смыслу. Группы должны быть осмысленными, и их имена должны отражать их назначение. В названии группы Sales (Продажи) не много пользы, а вот название наподобие SalesPrintOnly (Печать только для группы продаж) очень информативно. Вы должны создавать группы так, чтобы разделить пользователей по назначению, уровню доступа, задачам, подразделениям или любым другим важным аспектам. Помните, что группы существуют для того, чтобы облегчить вам жизнь, так что старайтесь извлечь из них максимум пользы.

Снабдите своих пользователей профилем

Профиль пользователя (user profile) — это совокупность рабочего стола, окружения, сети и других установок, которые определяют и контролируют стиль функционирования рабочей станции или рядового сервера. Сервер Windows Server 2003 записывает информацию о профиле автоматически для каждого пользователя. Однако до тех пор, пока вы не создадите для них перемещаемые профили (которые рассматриваются позже в этой главе), эти профили доступны только локально.

Профиль пользователя содержит большой объем информации об окружении и о деятельности пользователя, включая следующие сведения.

- ✓ Конфигурация меню Start (Пуск).
- ✓ Установки для "хранителя экрана" и "обоев".
- ✓ Перечень документов, используемых последними.
- ✓ Список Favorites для Internet Explorer.
- ✓ Сетевые отображения устройств.
- ✓ Установленные сетевые принтеры.
- ✓ Схема рабочего стола.

Кроме того, профиль включает сжатую копию ключей системного реестра HKEY_CURRENT_USER в файле NTUSER.DAT. Чтобы найти определения для всех различных ключей системного реестра, воспользуйтесь утилитой Registry из Tool в Resource Kit для Windows Server 2003 и обратитесь к файлу REGENTRY.HLP.

Вы можете превратить профили в перемещаемые профили. (Неперемещаемый профиль называется *локальным профилем.) Перемещаемый профиль (roaming profile)* — это профиль, который хранится в устройстве, доступном из сети; таким образом, независимо от того, какая рабочая станция используется для получения доступа, пользовательский профиль доступен. В результате рабочая среда пользователя следует за ним с одного компьютера на другой. (Вы также можете установить профиль таким образом, чтобы пользователь не смог настроить свой перемещаемый профиль, который называется обязательным профилем пользователя — Mandatory User Profile.) Подробно об этом рассказывается ниже в этом разделе.

Чтобы создать и включить перемещаемый профиль для определенного пользователя, выполните следующее.

1. **На контроллере домена создайте общедоступный каталог и присвойте ему имя User (или любое другое).**
2. **На рабочей станции, где расположен существующий локальный профиль, в окне Control Panel (Панель управления) выберите пиктограмму System (Система).**
3. **Щелкните на вкладке User Profiles (Профили пользователей).**
4. **Выберите профиль, который вы намерены превратить в перемещаемый.**
5. **Щелкните на кнопке Copy To (Копирование профиля).**
6. **Определите путь для нового места хранения профиля, доступный из сети.**

   Например, `\\domain controller\users\<имя пользователя>`, где `domain controller` — имя контроллера домена; `users` — имя сетевой папки; `<имя пользователя>` — имя учетной записи пользователя, связанной с профилем.
7. **На контроллере домена (или на любой другой машине домена, на котором надлежащим образом установлены средства ADMINPAK.MSI) запустите утилиту Active Directory Users and Computers (выбрав команду Start⇨All Programs⇨Administrative Tools⇨Active Directory Users and Computers (Пуск⇨Программы⇨Администрирование⇨Active Directory — Пользователи и компьютеры)).**
8. **Щелкните правой кнопкой мыши на объекте пользователя, который вы только что скопировали на контроллер домена, и выберите пункт меню Properties (Свойства).**
9. **Щелкните на вкладке Profile (Профиль).**
10. **В диалоговом окне Profile Path (Путь к профилю) раздела User Profile (Профиль пользователя) введите тот же путь, что и на шаге 6.**
11. **Щелкните на кнопке OK.**

Теперь профиль для выбранного пользователя — перемещаемый. После задания для пользователя перемещаемого профиля локальный профиль не используется. Он остается в системе, но теперь учетная запись пользователя связана с перемещаемым профилем.

По умолчанию всякий раз, когда пользователь выходит из системы, все изменения в его профиле, внесенные в ходе сеанса (независимо от того, какую рабочую станцию он использовал), сохраняются в его профиле на контроллере домена, пока вы не превратите его в обязательный профиль. При следующем входе пользователя в систему рабочая среда в точности повторяет ту среду, которая была при его выходе из системы. Локальные и перемещаемые профили должны использоваться только для одного пользователя. Если нескольким пользователям требуется один и тот же профиль, вы можете задействовать обязательный профиль.

Обязательный профиль (mandatory profile) не сохраняет индивидуальных или личных изменений, вносимых в профиль при выходе пользователя из системы. Профиль постоянно хранит одну и ту же конфигурацию. Этот тип профиля используется в основном, когда администраторы системы или сети намерены контролировать или ограничить возможности конечных пользователей по изменению их профилей по сравнению со стандартным, который может применяться в пределах всего предприятия.

Обязательный профиль легко создать, переименовав файл NTUSER.DAT в NTUSER.MAN в локальном либо в перемещаемом профиле. После такого изменения профиль остается состоятельным, независимо от того, кто его использует. Вы можете всегда отменить эти действия, переименовав файл NTUSER.MAN в NTUSER.DAT.

Политики групп

Политики групп (group policies) — это совокупность правил управления, контроля и наблюдения за действиями пользователей. Вы можете установить политики групп на базе сетевых узлов, доменов или производственных подразделений. В системе Windows NT Server 4.0 соответствующие средства были известны как System Policy Editor (Редактор системной политики). В Windows Server 2003 (так же как и в Windows 2000) вы устанавливаете все эти политики, используя политику групп и ее расширений встроенных утилит, таких как Administrative Templates, Security Settings, and Scripts (Шаблоны, параметры безопасности и сценарии администрирования).

Один из способов администрирования (управления или модификации) политики групп с помощью консоли Active Directory Users and Computers состоит из следующих действий.

1. **Запустите консоль Active Directory Users and Computers .**
2. **Щелкните правой кнопкой мыши на контейнере домена или производственного подразделения, для которых вы намерены установить политику,** а **затем выберите пункт меню Properties (Свойства).**
3. **Щелкните на вкладке Group Policy (Групповая политика).**
4. **Если вы намерены модифицировать существующую политику группы, выделите ее в области Group Policy Object Link (Ссылки на объем групповой политики) диалогового окна и выберите соответствующую опцию. На вкладке Group Policy доступны следующие опции (мы приводим их в алфавитном порядке).**

- ✓ **Add (Добавить).** После выбора этой опции открывается диалоговое окно Group Policy Object Link. Если вы хотите добавить существующий объект политики групп к домену или производственному подразделению, которые вы просматриваете, можете выполнить эту операцию в рамках этой опции.
- ✓ **Block Policy Inheritance (Блокировать наследование политики).** Эту опцию следует выбрать, чтобы запретить выбранному вами объекту каталога наследовать политику групп от родительского каталога.
- ✓ **Delete (Удалить).** Используйте эту опцию, если вы намерены удалить объект политики групп.
- ✓ **Edit (Изменить).** Позволяет внести изменения в выбранную групповую политику.
- ✓ New **(Создать).** Позволяет создать новый объект политики групп.
- ✓ **Properties (Свойства).** Позволяет открыть диалоговое окно Group Policy Properties. Используя выбранную политику, вы можете отыскать все сетевые узлы, производственные подразделения и домены. Кроме того, вы можете установить разрешения на доступ к этому объекту на базе пользователя или группы.

На вкладке Group Policy расположена кнопка Options. Щелкнув на этой кнопке, вы можете воспользоваться следующими возможностями.

- Disabled (Отключить). Временно отключает политику групп от объекта каталога.
- **No Override (Не перекрывать).** Эта опция подобна наложению вето. После выбора этой опции дочерние каталоги ***должны*** наследовать групповую политику от их родительского каталога. Даже параметр Block Policy Inheritance не может предохранить эту групповую политику от принудительного наследования после установки флажка No Override.

Если в списке политик представлено более одного объекта политики групп, воспользуйтесь кнопками Up (Вверх) и Down (Вниз), чтобы изменить порядок применения политик групп. Политики приводятся в действие по списку снизу вверх. Политика, которая находится вверху списка, приводится в действие последней и поэтому обладает преимуществом над всеми другими политиками в списке или любыми другими объектами, которые обрабатываются на более высоких уровнях схемы наследования, например уровень родительского производственного подразделения, домена или узла

Политики групп обрабатываются в следующем порядке.

1. Системы Windows 2000, Windows XP Professional и Windows Server 2003 обладают одним объектом политики локальной группы, и при запуске системы он обрабатывается первым. В сценарии с доменом этот объект политики групп скорее всего будет в наименьшей степени влиять на локальную систему, которая входит в домен, поскольку последующие объекты политики групп, вероятно, замещают эти параметры. В автономных системах Windows обычно обрабатывается только один объект политики групп. В этой ситуации он будет обладать наибольшим, если не единственным, влиянием.
2. Следующим набором параметров политики групп, подлежащим обработке, являются параметры для всех объектов политики групп узлов. Эти объекты политики групп обрабатываются синхронно (администраторы доменов устанавливают порядок, в котором выполняется их обработка). Они обрабатываются в соответствии со списком снизу вверх, при этом одна из них на самом верху списка вступает в действие последней на этом уровне.
3. После того как все политики групп для узлов задействованы, следующим развертывается набор объектов политик групп на уровне домена. Эти политики также выполняются синхронно и обрабатываются снизу вверх по списку, при этом одна из них на самом верху списка вступает в действие последней, если развертыванию подлежит больше одного набора.
4. Последним должен быть выполнен набор объектов политик групп уровня производственных подразделений. Все объекты политик групп, связанные с самым верхним (родительским) производственным подразделением в дереве наследования, выполняются первыми, за ними следуют те, которые расположены на следующем более высоком уровне, и так до тех пор, пока вы не достигнете локального производственного подразделения, политика которого применяется последней. Для каждого производственного подразделения в иерархии может существовать несколько политик. Они обрабатываются в определенном порядке, который устанавливается администратором домена и выполняются синхронно. Это означает, что все объекты политики групп в самой верхней точке дерева наследования выполняются первыми в определенном порядке, который устанавливается администратором домена, после чего все объекты политики групп, расположенные в следующей точке иерархии дерева наследования, выполняются в определенном порядке, устанавливаемом администратором домена, и т.д. по всему пути сверху вниз, вплоть до локального производственного подразделения.

При наличии противоречивых установок применяются два правила. Для любого конкретного объекта политики групп (Group Policy Object — GPO) установки компьютера превалируют над установками пользовательской конфигурации. Например, если объект GPO3, расположенный внизу списка, установленного на уровне домена, имеет параметры конфигурации компьютера, заданные таким образом, чтобы выполнять одни действия, а пользовательский раздел того же объекта политики групп установлен для выполнения противоположных действий, для использования будут разрешены параметры, приведенные в компьютерной конфигурации. Второе правило заключается в том, что все действия, выполняемые следующими, обладают преимуществом. В продолжение предыдущего примера это правило формулируется так: если следующий объект политики групп, установленный на уровне домена (GPO2), имеет другие установки, которые противоречат предыдущим (GPO3), то первенство остается за этим следующим объектом политики групп.

Приведем пример.

1. Объект GPO локальной системы предписывает удалить пункт RUN (Выполнить) из меню Start (Пуск). (Он удаляется.)
2. Объект GPO2 на уровне домена (расположенный внизу списка) предписывает удалить пункт RUN из меню Start. (Он удаляется.) Объект GPO1 на уровне домена (расположенный вверху списка) предписывает включить пункт RUN в меню Start. (Он добавляется.)
3. Объект GPO2 на родительском уровне производственного подразделения (расположенный внизу списка) предписывает включить пункт RUN в меню Start. (Он добавляется.) Объект GPO1 на родительском уровне производственного подразделения (расположенный вверху списка) предписывает включить пункт RUN в меню Start. (Он добавляется.)
4. Объект GPO3 на уровне локального производственного подразделения (расположенный внизу списка) предписывает включить пункт RUN в меню Start. (Он добавляется.) Объект GPO2 на уровне локального производственного подразделения (расположенный в середине списка) предписывает включить пункт RUN в меню Start. (Он добавляется.) Объект GPO1 на уровне локального производственного подразделения (расположенный вверху списка) предписывает удалить пункт RUN из меню Start. (Он удаляется.)

Вы можете спросить: "Что все это значит?" Пример политики, который мы рассмотрим в следующем разделе, проведет вас через процесс установки политики.

Создание групповой политики

Предположим, что вы намерены установить политику групп, применимую ко всем пользователям домена. Политика должна препятствовать пользователям изменять свой пароль. Чтобы реализовать новую политику групп, выполните следующее.

1. **Запустите консоль Active Directory Users and Computers.**
2. **Щелкните правой кнопкой мыши на контейнере домена или производственного подразделения, для которых вы намерены установить политику, а затем выберите пункт меню Properties.**
3. **Щелкните на вкладке Group Policy.**
4. **Щелкните на кнопке New (Создать), введите имя для политики, а затем нажмите клавишу <Enter>.**

5. **В разделе Group Policy Object Link выделите новую политику и щелкните на кнопке Edit (Изменить).**
6. **Проследуйте по пути вниз через левую панель окна до объекта User Configuration⇨Administrative Templates⇨System⇨Ctrl+Alt+Del Options (Конфигурация пользователя⇨Запретить Административные шаблоны⇨Система⇨Опции Ctrl+Alt+Del), как показано на рис. 15.7.**
7. **Дважды щелкните мышью на объекте Remove Change Password (Устранить замену пароля) в правой панели.**
8. **На вкладке Policy установите переключатель Enabled (Разрешить), щелкните на кнопке Apply (Применить), а затем на кнопке OK.**

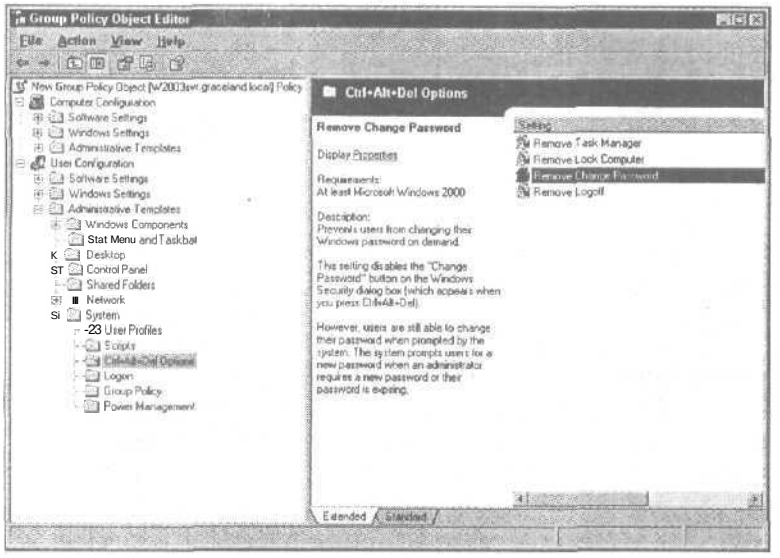


Рис. 15.7. ***Опции*** *Ctrl+Alt+Del, которые можно установить с помощью административного шаблона пользовательской конфигурации*

Эта новая политика влияет на все текущие и будущие учетные записи пользователей в домене, поскольку она была создана в контейнере домена и связана с ним. Однако она не влияет на те учетные записи, которые подключены к системе. Для них новая политика вступит в силу после того, как они выйдут из системы и вновь войдут в нее.

Обратите внимание, что когда вы переходите на вкладку Group Policy и щелкаете на кнопке Edit, на экране отображается информация, относящаяся к конфигурации компьютера, а также пользовательская конфигурация. Если между ними существует противоречие, в Windows Server 2003 преимущество остается за конфигурацией компьютера.

Предыдущие шаги позволили вам добавить политику групп, а затем отредактировать политику с помощью шаблонов Administrative Templates, которые видны вам. Другие шаблоны доступны, но просто не загружены. Чтобы добавить еще один шаблон, вернитесь к левой панели окна: под объектом User Configuration найдите объект Administrative Templates и щелкните на нем правой кнопкой мыши. Затем выберите пункт меню Add/Remove Templates (Добавить/Удалить шаблоны), чтобы отобразить список политик. Щелкните на кнопке Add, чтобы просмотреть другие имеющиеся в наличии шаблоны.

В папке Computer Configuration⇨Windows Settings⇨Security Settings (Конфигурация компьютера⇨Параметры Windows⇨Параметры безопасности) вы обнаружите немало полезных политик с заранее настроенной для вас конфигурацией (рис. 15.8). Например, существует шаблон для установления политики, которая предписывает использование уникальных паролей для учетных записей.

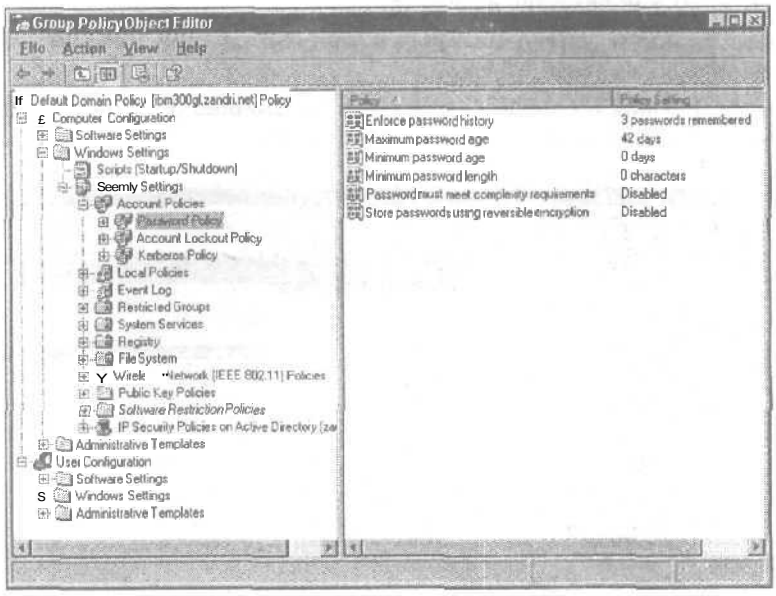


Рис. 15.8. Список групповых политик, которые можно применить на базе конфигурации компьютера

Если вы озабочены обеспечением безопасности, применяйте политику учетных записей, которая требует регулярного изменения паролей (новый пароль должен вводиться каждые 30 дней) и блокирует учетные записи, которым не удалось успешно войти в систему после трех попыток.

Аудит нарушений

Чтобы получить информацию о контроле доступа для любой заданной политики групп, вы можете проверить, какие объекты системы связаны с политикой, кто имеет разрешение на политику и каким образом она подвергается аудиту (именно к последнему вопросу мы обратимся в этом разделе). Для этого щелкните на кнопке Properties диалогового окна Group Policy.

Аудит информации в сети позволяет отслеживать действия в пределах всей сети. Этот процесс может помочь обнаружить проблемы конфигурации, попытки взлома системы защиты, неверные действия и неправильное использование системы. Чтобы сделать возможным аудит вашей локальной системы, выполните следующие действия.

1. **В диалоговом окне Group Policy щелкните на кнопке Properties.**
2. **В разделе Administrative Tools (Администрирование) выберите команду Local Security Policy (Локальная политика безопасности).**
3. **Переместитесь по левой панели до объекта Security Settings⇨Local Policies (Параметры безопасности⇨Локальные политики), затем щелкните на объекте Audit Policy (Политика** аудита).

4. **Дважды щелкните мышью на опции, которую вы намерены подвергнуть аудиту.**

   Появится диалоговое окно Security Settings (Параметры безопасности).

5. **Выберите возможность аудита, которой вы желаете воспользоваться: аудит успешных попыток или аудит неудачных попыток.**

   (В этом диалоговом окне администратор может выбрать возможность аудита успешных попыток, неудачных попыток или тех и других.)

6. **После того как вы сделаете выбор, щелкните на кнопке OK.**

Наиболее полезно проводить аудит неудачных попыток для определенных объектов, таких как попытки входа в систему и доступа к объектам. Это может служить вам предупреждением об угрозе несанкционированного вторжения в систему.

Информация, полученная посредством аудита, записывается в журнале Security Log (Журнал безопасности) приложения Event Viewer (Просмотр событий). Запустите приложение Event Viewer из меню Administrative Tools (Администрирование) и выберите узел Security Log. Правая панель отображает список элементов, выбранных вами для аудита. Регулярно проверяйте этот журнал, а затем очищайте его, чтобы он не переполнялся.

Следует напомнить еще об одном моменте: эти примеры используют локальную политику безопасности. Если политика домена отличается от локальной политики, то преимущество остается за политикой домена. Например, если вы установили регистрацию всех успешных и неудачных действий для всех элементов локальной политики безопасности, а политика безопасности домена установлена в Not Configured (Не конфигурировать), никакая регистрация не будет разрешена, поскольку политика безопасности домена вступает в действие после локальной политики безопасности.

Если возникнут проблемы доступа...

Учетные записи пользователей определяют круг лиц, которые могут получить доступ к компьютерной системе, а также уровень доступа, которым они обладают. Тем не менее иногда пользователи сталкиваются с проблемами, которые препятствуют нормальному прохождению процесса входа в систему.

Поскольку большая часть проблем входа в систему возникает при неверном вводе пароля, пользователи должны уделять вводу своих паролей достаточно времени. Этот совет придется кстати только в том случае, если их учетные записи не заблокированы из-за неудачных попыток входа в систему. Если пользовательская учетная запись заблокирована, ее следует установить заново. Это можно выполнить двумя способами. Если политика блокирования установлена на определенное время, вам необходимо просто дождаться, пока время не истечет, и попытаться снова войти в систему. Если политика блокирования требует административного вмешательства, переустановите эту учетную запись пользователя.

Если пользователь не может войти в систему или взаимодействие с сетью выглядит спорадическим, выполните следующее.

- ✓ Убедитесь в том, что карта сетевого адаптера и другие физические сетевые соединения надежно установлены.
- ✓ Для любой Windows-системы — Windows NT Workstation, Windows 2000, Windows XP Professional или Windows Server 2003 — вы должны убедиться в том, что компьютер является членом домена, чтобы иметь возможность войти в домен с учетной записью, каталогизированной в Active Directory, для доступа к сетевым ресурсам.

- ✓ При использовании протокола IP и статически присвоенных IP-адресов проверьте параметры конфигурации, чтобы гарантировать, что компьютер использует корректный IP-адрес, маску подсети и шлюз по умолчанию, и убедитесь в том, что он обладает надлежащими параметрами DNS для сети.
- ✓ Если в вашей сети применяется протокол DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации узла) для задания параметров IP-адресации компьютеров — от небольшой совокупности до большой группы, — вы можете оказаться в ситуации, когда все доступные адреса соединений находятся в использовании. Вы можете проверить, не случилось ли это, прибегнув к помощи приглашения для ввода командной строки, введя команду IPCONFIG/ALL и просмотрев параметры. Если ваш IP-адрес попадает в диапазон 169.254.0.1-169.254.254.254 для автоматических частных IP-адресов (Automatic Private Internet Protocol Address — APIPA), возможно, что DHCP-сервер вышел за пределы допустимых адресов либо в системе возникли проблемы взаимодействия с DHCP-сервером.

Если пользователи могут войти в систему, но не могут получить доступ к ресурсам, которые, как они полагают, должны быть им доступны, проверьте следующее.

- ✓ Принадлежность к группам.
- ✓ Физические сетевые соединения с узлами, на которых распложены ресурсы (т.е. проверьте, не отсоединился ли сетевой кабель сервера).
- ✓ Наличие политик групп, ограничивающих действия пользователей.

Если все, о чем мы упомянули, проверено, вы имеете дело с чрезвычайно таинственной проблемой. В поисках решения обратитесь к ресурсам Microsoft (в интерактивном режиме или через TechNet). Ясное дело, что это не лучший совет, однако это самое стоящее, что мы можем предложить. Информационная база Microsoft обширна — если кто-либо еще сталкивался с подобной проблемой, вы, вероятно, сможете отыскать присланную информацию о ее решении.

Глава 16

Управление разрешениями

В этой главе...

- Объекты, права и разрешения
- Применение разрешений к NTFS-объектам
- Разделы FAT и FAT32
- Применение разрешений к разделяемым файлам
- Определение действующих разрешений
- Работа по управлению доступом

В значительной мере работа с Windows Server 2003 означает использование файловой системы Windows NT, которая больше известна как NTFS (Windows NT File System). Развитые возможности этой системы включают списки ACL (Access Control List — список контроля доступа) для объектов на уровне атрибутов, так что вы можете не только управлять доступом к тому, каталогу или файлу со стороны пользователей или групп, но также контролировать операции, которые пользователи или группы могут выполнять над этим томом, каталогом или файлом.

Windows 2003 также поддерживает файловые системы FAT и FAT32 (FAT — *File Allocation Table* (таблица размещения файлов)), которые не включают элементы управления доступом на уровне объектов. Однако файловые системы FAT и FAT32 поддерживают так называемые *совместно используемые файловые ресурсы (file shares)* (совместно используемые каталоги с файлами, которые они содержат), поддерживающие элементы управления доступом. Основная цель данной главы — объяснить, как работают совместно используемые ресурсы и как разрешения файловой системы NTFS сочетаются с разрешениями на совместно используемые ресурсы. Мы покажем, как определить, что пользователь может (и что не может) делать с вашими файлами исходя из разрешения его учетной записи, группы, к которой он принадлежит, и основополагающих принципов умолчания применительно к самой системе Windows Server 2003.

В главе 12 эта информация рассматривалась применительно к Active Directory.

Еще об объектах, правах и разрешениях

Прежде чем вы углубитесь в подробности, касающиеся прав и разрешений применительно к Windows 2003, вам следует усвоить некоторые термины. Вот почему мы совершим небольшой экскурс в страну слов — прямо здесь, прямо сейчас.

Урок по объектам

Windows 2003 трактует все доступные пользователю системные ресурсы — включая пользователей, группы, файлы, каталоги, принтеры и процессы — как объекты. Термин *объект* (*object*) имеет для программистов специальный смысл: под этим термином понимают именованную совокупность атрибутов и значений, а также именованную совокупность методов, которые Microsoft называет *службами (service)*.

Например, объект-файл обладает различными атрибутами, о которых вы уже знаете, если провели некоторое время возле компьютеров: файлы имеют имя, тип, размер, владельца, а также даты создания и модификации. Что касается объекта, то каждый атрибут также обладает связанным с ним значением; следовательно, для файла перечень возможных атрибутов и значений может выглядеть следующим образом.

- ✓ Name (Имя). BOOT.INI.
- ✓ Type (Тип). Параметры конфигурации.
- ✓ Contents (Содержимое). Информация, касающаяся загрузки Windows 2003. (Windows 2003 может устанавливать местоположение и считывать содержимое, используя дисковый каталог файлов.)
- ✓ Size (Размер). Приблизительно 1 Кбайт.

Атрибуты идентифицируют отдельные объекты некоторого специфического типа — в данном случае типа "файл" — и определяют, что они содержат, где расположены и т.д.

С другой стороны, ответ на вопрос, почему методы или услуги важны для объектов, может оказаться и не столь очевидным. Если вы исследуете файловый объект, то можете понять, что его метод описывает операции, которые вы желаете применить к файлу. Поэтому методы или услуги, применимые к объекту-файлу, включают такие операции, как чтение, запись, выполнение, удаление, переименование и другие типичные файловые операции. Короче говоря, методы определяют операции, которые можно применить к конкретному объекту. Помимо прочего, объекты в значительно большей мере становятся самоопределяемыми, поскольку они включают в свои атрибуты полное описание самих себя, а также включают в свои методы полное описание того, что вы можете делать с ними. Другие типы объектов обладают другими связанными с ними методами или службами, которые отражают возможности объектов и данные, содержащиеся объектах.

Рассмотрение атрибутов специфических объектов в Windows 2003 может вызвать неподдельный интерес. Каждый единичный атрибут и отдельный объект обладают ACL-списком. ACL-списки идентифицируют те отдельные учетные записи пользователей или группы, которые могут осуществлять доступ к конкретному объекту (или одному из их атрибутов), а также указывают на то, какие службы каждый пользователь или группа могут применить к этому объекту (или одному из его атрибутов). Администраторы используют ACL-списки для управления доступом к объектам (и, логически рассуждая, к их атрибутам), что освобождает их от необходимости заниматься поиском проблем с объектами за счет ограничения возможностей рядовых пользователей случайно (или преднамеренно) повредить систему.

Когда файл не является объектом

Система Windows 2003 применяет понятие объекта практически ко всему в ее операционной среде, к чему пользователи могут получить доступ. Фактически тома, каталоги и файлы файловой системы NTFS представляют собой объекты Windows 2003 со связанными с ними атрибутами и набором определенных служб, которые можно приложить к этим объектам. Но поскольку устаревшая файловая система FAT (как и сравнительно более новая файловая система FAT32 для Windows 98) не включает встроенную поддержку для ACL, файлы FAT и FAT32 *не являются* объектами. Поэтому, несмотря на то, что тома, каталоги и файлы FAT и FAT32 по-прежнему обладают атрибутами, аналогичными атрибутам файлов NTFS (а именно: именем, типом, датой создания, датой модификации и т.д.), тома, каталоги и

файлы FAT и FAT32, по существу, не являются объектами. Отсутствие встроенной поддержки для ACL объясняет, почему тома FAT и их содержимое не защищены (потому что обычные разрешения к ним не применимы).

Что более важно, это также объясняет, почему используемые по умолчанию сценарии входа в систему Windows Server 2003 ни за кем не признают права на локальный вход в систему, кроме администраторов, операторов серверов, операторов резервного копирования и операторов принтеров. Это связано именно с тем фактом, что любой, кто получил доступ к тому FAT или FAT32, может делать все, что ему заблагорассудится. Отвергая право рядовых пользователей на вход в систему Windows Server 2003 с помощью клавиатуры и требуя от них входа только через сеть, Windows 2003 может контролировать доступ к томам Server через совместно используемые ресурсы. Совместно используемые ресурсы работают как объекты Windows 2003 и, следовательно, обладают встроенными элементами управления доступом.

Пользователи обладают правами, а объекты — разрешениями

В соответствии со стандартной терминологией, принятой в Windows 2003, говорят о *правах пользователя (user right) и разрешениях объектов (objectpermission)*. Поскольку понятие разрешений объекта довольно неопределенное, обычно говорят о разрешениях, используемых применительно к определенным классам объектов, таких *как разрешения файлов* и *разрешенияпринтеров*.

Права пользователя определяют, что он может делать с объектом (или его атрибутами) в среде Windows 2003. Пользователь получает права на объект одним из трех способов.

- ✓ Права явно присваиваются отдельной учетной записи пользователя.
- ✓ Права присваиваются группе, к которой принадлежит пользователь. Именно таким образом пользователю предоставляются полномочия на выполнение определенных задач, например резервного копирования файлов и каталогов.
- ✓ Права присваиваются с помощью окна Group Policy (Групповая политика). Чтобы получить доступ к этому окну, откройте одно из окон администрирования Active Directory (Administrative tools), щелкните правой кнопкой мыши на пиктограмме узла, производственного подразделения, домена или локального компьютера. Выберите элемент меню Properties (Свойства), выберите вкладку Group Policy, а затем щелкните на кнопке Edit (Редактировать). Отредактируйте права пользователя в окне Group Policy, выполнив команду Computer Configurations⇨Windows Settings⇨Security Settings⇨Local Policies⇨User Rights assignment (Конфигурация компьютера⇨Параметры Windows⇨Параметры безопасности⇨Локальные политики⇨Назначение прав пользователя).

Когда пользователь входит в домен Windows 2003 (или в автономную систему), генерируется специальный ключ, который называется *маркером доступа (access token)*. Маркер доступа представляет явные личные права пользователя и группы, к которым пользователь принадлежит. На генерацию маркера доступа уходит некоторое время, и это одна из причин того, что регистрация при входе в Windows 2003 происходит не мгновенно.

Каждый объект (и его атрибуты) в среде Windows 2003 включает атрибут, называемый *разрешения (permissions)*(который можно найти во вкладке Security (Безопасность) каждого объекта)). Этот атрибут разрешений включает ACL-список, идентифицирующий всех пользователей и группы, которым разрешен доступ к атрибутам объекта, а равно и ко всем службам, которые каждый пользователь или группа могут применить к атрибутам объекта. Всякий раз, когда пользователь запрашивает объект, Windows 2003 использует встроенную функцию Security Reference Monitor (SRM) (Контрольный монитор безопасности), чтобы сравнить маркер

доступа пользователя с разрешениями для этого объекта. Если SRM-монитор устанавливает, что пользователь имеет разрешение, Windows 2003 выполняет запрос; в противном случае пользователю не повезет. Для пользователей существует возможность получить доступ лишь к определенным атрибутам объекта, в то время как доступ к другим атрибутам им не будет разрешен. Например, Нанси может быть предоставлен доступ для просмотра части учетной информации Джоан, такой как ее телефонный номер, но не к адресу Джоан.

Файловая система NTFS Windows 2003 и разрешения

Файловая система NTFS во многом похожа на файловые системы FAT и FAT32 (32-разрядная таблица размещения файлов, используемая в Windows 98). Различие между NTFS и этими файловыми системами состоит в том, что NTFS — *объектно-ориентированная файловая система.* В отличие от FAT и FAT32 файловая система NTFS представляет себе все в NTFS-разделах как объекты некоторого определенного типа, которые обладают атрибутами и к которым могут применяться методы и службы. Преимущество использования NTFS заключатся в том, что вы можете установить разрешения для томов, файлов и каталогов, которые используют NTFS.

Фактически файловая система NTFS распознает три типа объектов.

- ✓ Тома. Раздел диска в формате NTFS, который отображается в виде пиктограммы дискового устройства. Объект-том может содержать файлы и каталоги.
- ✓ Каталоги. Поименованный контейнер для файлов, который содержится внутри тома или каталога. Фактически Windows 2003 позволяет использовать вложенные каталоги произвольной глубины; это означает, что вы можете поместить столько каталогов внутри каталогов, сколько пожелаете (хотя уровни вложенности каталогов чрезвычайно быстро исчерпываются).
- ✓ Файлы. Поименованный контейнер для данных, который, помимо прочих, включает такие атрибуты, как тип, размер, даты и содержимое, Именно в файлах NTFS фактически хранится информация.

Чтобы проверить разрешения для какого-либо объекта в NTFS, щелкните правой кнопкой мыши на этом объекте в окне Windows Explorer My Computer Active Directory Sites and services. В раскрывающемся меню выберите пункт Properties (Свойства), а затем щелкните на вкладке Security (Безопасность). В нижней части диалогового окна Security вы увидите раздел Permissions (Разрешения) (рис. 16.1). В этом разделе вы можете проанализировать список доступных разрешений для этого объекта (в нашем случае — том E на жестком диске) с помощью списка, который появляется в разделе Permissions в нижней части экрана.

Разрешения NTFS

Список Permissions отображает разрешения для объектов-файлов, объектов-томов и объектов-каталогов в файловой системе NTFS. Разрешения для файлов, томов и каталогов NTFS аналогичны. Единственные реальные отличия состоят в том, что объекты-контейнеры обеспечивают возможности наследования разрешений дочерними объектами, и немногие разрешения применяются только к контейнерам. Мы используем общий термин *контейнер (container)* применительно к томам и каталогам — другими словами, к объектам, которые ведут себя как родительские по отношению к дочерним.

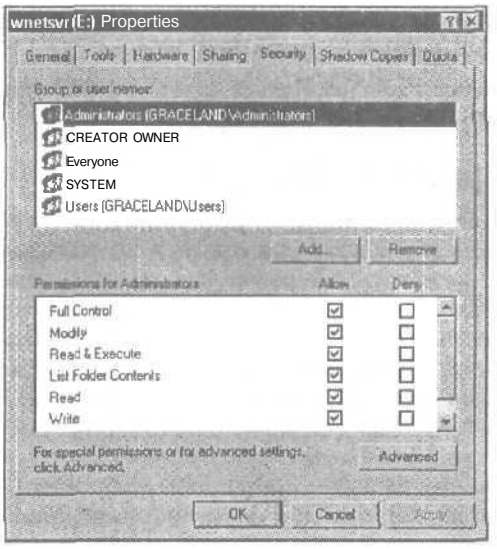


Рис. 16.1. Список разрешений, применимых к объекту

Метод назначения разрешений и ограничения разрешений в Windows 2003 немного отличается от подобных методов, используемых в Windows NT, однако полностью аналогичен методу, который используется в Windows 2000. Прежде всего, в Windows 2003 отсутствует разрешение No Access (Нет доступа). Вместо этого все разрешения либо предоставляются, либо ограничиваются с помощью параметров Allow (Разрешить) и Deny (Запретить). Выбор параметра Deny для всех возможных разрешений для объекта NTFS в среде Windows 2003 означает то же самое, что и параметр NO Access в Windows NT.

Вот перечень стандартных разрешений NTFS.

- ✓ **Read (Чтение).** Предоставляет пользователям возможность просматривать содержимое папки или файла.
- ✓ **Write (Запись)** (папки). Предоставляет пользователям возможность создавать новые папки и файлы внутри папки.
- ✓ **Write (Запись)** (файлы). Предоставляет пользователям возможность изменять содержимое файла и изменять его атрибуты.
- ✓ **List Folder Contents (Список содержимого папки)** (только папки). Предоставляет пользователям возможность просматривать имена содержимого папки.
- ✓ **Read & Execute (Чтение и выполнение)** (папки). Предоставляет пользователям возможность просматривать содержимое папки или файла и выполнять программы.
- ✓ **Read & Execute (Чтение и выполнение)** (файлы). Предоставляет пользователям возможность просматривать и выполнять программы.
- ✓ **Modify (Изменить)** (папки). Предоставляет пользователям возможность удалить папку и ее содержимое, создать новые файлы и папки внутри папки и просматривать содержимое папки.
- ✓ **Modify (Изменить)** (файлы). Предоставляет пользователям возможность удалить файл, изменить содержимое файла и его атрибуты и просматривать файл.

- ✓ Full Control (Полный доступ) (папки). Предоставляет пользователям неограниченный доступ ко всем функциям с файлами и папками.
- ✓ Full Control (Полный доступ) (файлы). Предоставляет пользователям неограниченный доступ ко всем функциям с файлами.

Дополнительные разрешения

Дополнительные разрешения (Advanced permissions) представляют собой элементы управления, которые можно использовать для создания специальных прав доступа в тех случаях, когда стандартное предоставление разрешений не применимо надлежащим образом. Доступ к дополнительным элементам управления можно получить, щелкнув на кнопке Advanced (Дополнительно) вкладки Permissions объекта NTFS. Откроется диалоговое окно Advanced Security Settings (Дополнительные параметры безопасности) с четырьмя вкладками: Permissions, Auditing (Аудит), Owner (Владелец) и Effective Permissions (Действующие разрешения). Вкладка Permissions используется для определения специальных разрешений, Auditing — для определения схемы аудита, вкладка Owner — для просмотра текущего владельца объекта. Вкладка Effective Permissions отображает разрешения, назначенные пользователю или группе по отношению к текущему объекту исходя из всех применимых параметров разрешения.

На вкладке Permissions можно добавить пользователя или группу и определить для них специальные разрешения. Ниже перечислены допустимые варианты выбора.

- ✓ Full Control (Полный доступ).
- ✓ Traverse Folder/Execute File (Обзор папок/Выполнение файлов).
- ✓ List Folder/Read Data (Содержание папки/Чтение данных).
- ✓ Read Attributes (Чтение атрибутов).
- ✓ Read Extended Attributes (Чтение дополнительных атрибутов).
- ✓ Create Files/Write Data (Создание файлов/Запись данных).
- ✓ Create Folders/Append Data (Создание папок/Дозапись данных).
- ✓ Write Attributes (Запись атрибутов).
- ✓ Write Extended Attributes (Запись дополнительных атрибутов).
- ✓ Delete (Удаление).
- ✓ Read Permission (Чтение разрешений).
- ✓ Change Permission (Изменение разрешений).
- ✓ Take Ownership (Смена владельца).

Если вам действительно нужно раскопать все эти подробности, касающиеся специальных прав доступа, обратитесь к компакт-диску TechNet и документации Windows Server 2003 Resource Kit от Microsoft.

В файловых системах FAT и FAT32 разрешения отсутствуют

Поскольку в файловых системах FAT и FAT32, поддерживаемых Windows 2003 наряду с NTFS, отсутствует объектный механизм для связывания атрибутов с файлами и каталогами, файлы, хранимые в томе в формате FAT и FAT32, не обладают соответствующими разреше-

ниями. Любой, кому позволено входить в систему Windows Server 2003, используя раздел FAT или FAT32, может получить доступ к файлам в этом разделе. Это помогает объяснить, почему вам может потребоваться ограничить разрешения для работы с вашим сервером и почему вы должны физически закрывать ваш сервер, попросту говоря, запирать его на замок,

Причина, по которой в современных системах все еще встречаются разделы FAT, состоит в том, что машины с двойной загрузкой, на которых совместно функционируют как Windows *9x,* так и Windows Server 2003, должны включать раздел FAT, с которого может загрузиться операционная система. Это может быть раздел FAT32 для Windows 98, но мы рекомендуем использовать FAT, поскольку Windows 2003 в процессе работы может читать этот раздел, и, кроме того, раздел FAT могут читать больше операционных систем, чем любой другой тип файловой системы.

Владение объектами в системе NTFS

Владелец объекта может всегда модифицировать его разрешения, независимо от того, какие разрешения уже установлены для этого объекта. Этот тип разрешения существует, по меньшей мере отчасти, чтобы иметь возможность избежать ловушки параметра разрешения Deny (Запретить), в которую можно попасть, когда владелец объекта по ошибке установит разрешения для общей группы, например группы Everyone (Все) или Authenticated Users (Авторизованные пользователи). Эти две используемые по умолчанию группы рассматриваются более подробно в главе 18.

Если группе Everyone назначен параметр Deny для всех типов разрешений для объекта, эта группа включает всех, кто бы вознамерился получить доступ к этому объекту, До тех пор, пока администратор или создатель объекта (и его владелец по умолчанию) не сможет установить несколько менее жесткие ограничения на доступ к объекту, никто не сможет обратиться к этому объекту или любому содержащемуся в нем объекту.

Параметр Full Control (Полный доступ) играет важную роль, поскольку предоставляет владельцу объекта возможность изменить доступ к этому объекту, а также службы, применимые к объекту. По существу, параметр Full Control — это ваша палочка-выручалочка.

Только Windows 2003/XP/2000 и Windows NT могут читать разделы NTFS, так что будьте осторожны при изменении формата разделов на машинах с двойной загрузкой! Кроме того, Windows 2003/XP и 2000 используют NTFS версии 5. Windows NT по умолчанию использует NTFS версии 4, однако если вы примените для обновления этой ОС служебный пакет Service Pack 4 или старше, Windows NT модифицируется таким образом, что будет включать NTFS версии 5.

Разрешения для совместного доступа

Когда пользователи обращаются к файлам сервера Windows Server 2003, это обычно происходит посредством сети, особенно, если вы ограничили круг пользователей, которым разрешен вход на сервер и физический доступ к машине. Поэтому большинство пользователей, которые обращаются к файлам сервера Windows Server 2003, осуществляют это посредством *сетевого совместно используемого ресурса (network share)*; этот сетевой ресурс представляет собой каталог Windows Server 2003, присоединенный к сети для общего доступа.

Совместно используемые ресурсы также являются объектами для Windows 2003, так что к ним применимы разрешения. Список допустимых разрешений состоит из следующих трех элементов, управление которыми осуществляется с помощью того же метода разрешения/запрещения (Allow)/(Deny), что и для непосредственных разрешений в отношении объектов NTFS.

- ✓ **Read (Чтение).** Разрешает просмотр файлов в **разделяемом** каталоге, загрузку этих файлов через сеть и выполнение программ.
- ✓ **Change (Изменить).** Включает все разрешения типа Read, кроме того, допускает создание, удаление и изменение каталогов и файлов, входящих в разделяемый каталог.
- ✓ **Full Control (Полный доступ).** Включает ясе разрешения типа Change, кроме того, включает разрешение на изменение разделяемого каталога и смену владельца.

Для совместно используемых ресурсов не существует каких-либо разрешений для специального доступа. В табл. 16.1 сведены воедино все основные разрешения для общих ресурсов.

Таблица 16.1. Разрешения для совместного доступа и базовые разрешения

Файл	Read	Write	Execute	Delete	Change
Read	x		x		
Change	x	x	x	x	
Full Control	x	x	x	x	x

Если вам необходимо открыть содержимое раздела FAT системы Windows Server 2003 для сетевых пользователей, то выполнение этой задачи посредством общего ресурса автоматически даст вам некоторую степень контроля, что можно расценить как еще одно преимущество использования сети!

Для создания совместно используемого ресурса щелкните правой кнопкой мыши на пиктограмме каталога в окне программы My Computer или Explorer Windows 2003, а затем выберите пункт Sharing and Security (Доступ и безопасность). Появится окно Properties для этого каталога с выбранной вкладкой Sharing (Доступ), как показано на рис. 16.2.

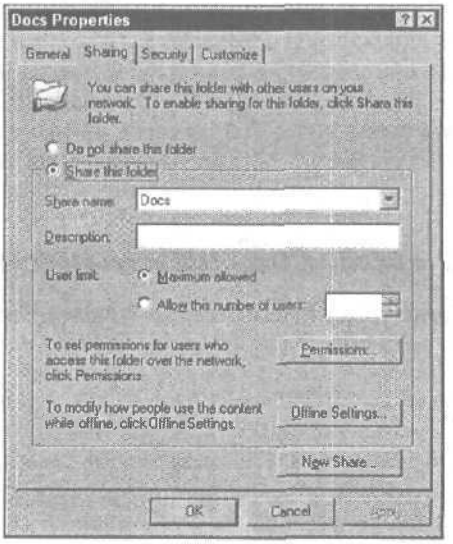


Рис. 16.2. Вкладка Sharing

Следующие элементы этого окна связаны с созданием и управлением общим ресурсом.

- **Share This Folder (Открыть общий доступ к этой папке).** Вы должны выбрать переключатель Share This Folder, чтобы разрешить общий доступ к каталогу или папке.
- **Share Name (Сетевое имя).** По умолчанию имя общего ресурса совпадает с именем каталога, которому он принадлежит. При создании общего ресурса помните о том, что пользователи DOS и Windows 3x могут обращаться к общему ресурсу только с помощью имен, не превышающих восьми символов.
- **User Limit (Предельное число пользователей).** Панель User Limit позволяет ограничить количество пользователей, которые могут одновременно обращаться к общему ресурсу. Обычно это имеет значение только для системы Windows Server 2003 с высокий нагрузкой; в большинстве случаев вы можете оставить для этого параметра значение, устанавливаемое по умолчанию, — Maximum allowed (Максимально возможное).
- **Кнопка Permissions (Разрешения).** Вы контролируете разрешения для совместного доступа посредством кнопки Permissions в правом нижнем углу вкладки Sharing. Эти разрешения работают аналогично разрешениям NTFS.
- **Кнопка Offline Settings (Автономные параметры).** Эта кнопка позволяет разрешить или запретить удаленным пользователям помещать содержимое этого общего ресурса в кэш на своей собственной машине с помощью окна Offline File and Folders. По умолчанию только файлы и программы, определенные пользователями, доступны в автономном режиме.

Вычисление действующих разрешений

Пользователи получают права не только как результат разрешений NTFS, явно назначаемых определенным файлам и каталогам для их учетных записей, но также в силу преимуществ групп, к которым они принадлежат. Поскольку существуют общие ресурсы NTFS, определение разрешений может приобрести значительный интерес, когда вы комбинируете разрешения NTFS и общих ресурсов для определенного файла или каталога, да еще если принять во внимание параметры пользователей и их членство в группах. Чтобы помочь вам определить истинное положение дел, мы предоставим правила вычислений, а также некоторые практические правила, а затем приведем пример, чтобы показать, как все это работает.

Правила вычислений

Чтобы вычислить, какие разрешения применены к общему ресурсу-объекту NTFS, вы должны, прежде всего, определить, какое разрешение применено в отношении самого объекта NTFS. Это может потребовать учета свойств наследования от родительского объекта к дочернему. (Чтобы освежить в памяти сведения о наследовании, обратитесь к главе 12.) Затем вы должны определить разрешения, примененные к общему ресурсу. (Правило для это процесса приведено в следующем разделе.) То из двух правил, которое является ограничивающим в большей степени, получает преимущество и определяет фактические разрешения, примененные к файлу или каталогу, о котором идет речь. Этот процесс несложен, но его результат может противоречить интуиции. Вы должны применять эти правила точно так, как они сформулированы, иначе мы не гарантируем правильность результата. Итак, начнем.

1. **Определите разрешения объекта.**
2. **Определите разрешения общего ресурса.**

3. **Сравните разрешения общего ресурса и объекта. Разрешение с *большей степенью ограничений* и есть применяемое разрешение.**

Всякий раз, когда вы или ваши пользователи не могут получить доступ к определенному объекту файловой системы посредством общего ресурса (или собственно NTFS, если на то пошло), проверяйте членство в группах и связанные ним разрешения.

Вычисли его!

Формальное объяснение может не полностью осветить процесс, поэтому в этом разделе мы приведем пару примеров.

Бетти принадлежит группам Marketing Dept (Отдел маркетинга), Domain Users (Пользователи домена) и Film Critics (Кинокритики). Она намерена удалить файл из общего ресурса NTFS под названием Rosebud.doc. Может ли она выполнить это? В табл. 16.2 приведены ее личные и групповые разрешения.

Таблица **16.2. Разрешения NTFS** и общего ресурса **для Бетти**

Тип	Членство	Имя	Разрешение
NTFS	Учетная запись пользователя	BettyB	Read
Группа	Marketing Dept		Read
Группа	Domain Users		Change
Группа	Film Critics		Change
Общий ресурс	Учетная запись пользователя	BettyB	Read
Группа	Marketing Dept		Read
Группа	Domain Users		Read
Группа	Film Critics		Read

С точки зрения NTFS, Read плюс Change равно Change; с точки зрения общего ресурса, Read — только забава. Из разрешений Read и Change большей степенью ограничения обладает разрешение Read. Итак, Read не позволит Бетти удалить файл, так что Бетти не повезло! Может быть, в следующий раз...

Пусть это сделает для вас ОС

Теперь, когда вы знаете, как вычислить разрешения вручную, мы расскажем вам о комбинации клавиш. На самом деле о ней уже говорилось в этой главе. Если вы отобразите диалоговое окно Advanced Properties из вкладки объекта Security, то сможете получить доступ к вкладке Effective Permissions. Если выбрать определенного пользователя или группу, на этой вкладке отобразятся действующие разрешения для этого пользователя или группы (рис. 16.3).

Управление доступом с помощью объектов Active Directory

Мы рассказали об объектах и управлении доступом, но что касается Active Directory, вам необходимо знать о двух дополнительных функциях делегирования управления доступом и наследовании на основе свойств. В следующем разделе описываются эти две функции в общем, а подробности содержатся в главе 12.

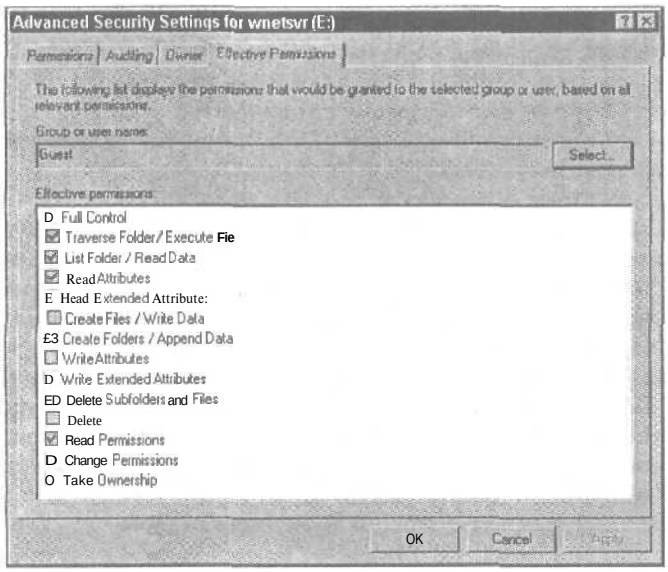


Рис. 16.3. ***Вкладка Effective Permissions***

Делегированиеуправлениядоступом

Вы можете позволить кому-нибудь другому управлять частью вашей сети за вас — иначе вы будете работать в режиме 24/7! В качестве базиса для разделения управления можно взять домен либо предоставить кому-то другому права на управление производственным подразделением вместо вас, в зависимости от функций, которые вы желаете на него возложить. Осуществить это можно с помощью мастера делегирования управления (Delegate Administration Wizard), которого можно вызвать из оснастки Active Directory Users and Computers. Выберите команду Start⇨Administration Tools⇨Active Directory Users and Computers, щелкните на пиктограмме домена, а затем выберите пункт Delegate Control из меню Action (Операции).

Производственное подразделение — это контейнер Active Directory, который содержит другие производственные подразделения, компьютеры, пользователей и группы. Более подробная информация о производственных подразделениях содержится в главе 11.

Прежде чем вы предоставите кому-то другому доступ к управлению объектами Active Directory, вы должны в первую очередь обладать надлежащими разрешениями на делегирование прав на этот объект. Кроме того, вы должны дать соответствующие разрешения другим на управление этим объектом.

Наследование на основе свойств

Так же как вы можете унаследовать деньги от своих родственников, более низкий уровень вашей сетевой структуры может унаследовать комплект информации об управлении доступом от более высокого уровня структуры. Наследование, как предполагает его название, всегда направлено сверху вниз. Мы хотим кратко рассказать о двух методах наследования на основе свойств. (Более подробную информацию о том, как работает этот метод наследования, можно почерпнуть из главы 12.)

Первый метод называется динамическим наследованием. Как предполагает слово *динамическое,* информация об управлении доступом для этого типа наследования вычисляется на лету всякий раз при запросе операций чтения/записи для этого объекта. Это приводит к некоторому увеличению нагрузки на сеть (такому как дополнительный трафик), которое следует принять во внимание для загруженных сетей. (Дополнительный трафик в загруженной сети может значительно замедлить ее работу.)

Второй метод называется *статической моделью,* известной также как *наследование в момент создания (Create Time Inheritance).* Это означает, что информация об управлении доступом для объекта устанавливается при создании объекта с помощью проверки разрешений родительского объекта и комбинирования этих разрешений с разрешениями нового объекта. До тех пор, пока новое разрешение не будет установлено на более высоком уровне, управление доступом для объекта остается неизменным. Поэтому при выдаче запроса на операцию чтения/записи для объекта нет необходимости выполнять какой-либо пересчет для определения разрешений. Однако, если разрешения изменяются на более высоком уровне, то они распространяются сверху вниз для изменения разрешений или повторной установки комбинированных разрешений на более низком уровне — аналогично опрокидыванию домино. Пересчет разрешений выполняется в единственном случае — при установлении разрешений и их распространении по иерархии сверху вниз, на более высоком уровне.

Глава 17

Запас на черный день

В этой главе...

- Почему так важно резервировать данные
- Планирование резервирования
- Обзор методов резервирования Windows Server 2003
- Раскрытие способов восстановления данных
- Поиск альтернатив, предлагаемых независимыми поставщиками
- Использование группы Backup Operators

Наличие схемы резервирования данных необходимо для жизненно важных бизнес-приложений и функций, которые обычно размещаются в сети. При отсутствии плана защиты данных вполне может произойти разрушение данных и нарушение производственных процессов всей организации, что приведет к потере дохода.

К сожалению, многие организации не слишком заботятся о защите своих данных до тех пор, пока им действительно не случится потерять их. В этой главе вы познакомитесь с различными методами защиты данных организации от возможной потери.

Резервирование данных

Резервирование (backing up) — это копирование данных из одного места хранения в другое, выполняемое либо вручную, либо автоматически. Копирование данных из одного каталога в другой на одном и том же жестком диске эффективно до тех пор, пока не произошел отказ жесткого диска и обе копии данных не стали недоступными. Кроме того, при копировании данных на тот же диск вы пренебрегаете копированием какой-либо информации, касающейся системы защиты и учетных записей. Это значит, что вы должны вводить эту информацию вручную. Не кажется ли вам, что лучше создать резервную копию всех файлов, содержащих системные, прикладные и пользовательские данные, на другой физический носитель, такой как магнитная лента или другое резервное устройство, а затем периодически сменять их по очереди вне системы?

Многие организации размещают в сети свои жизненно важные для бизнеса функции и данные: электронную почту, информацию об учетных записях, платежные ведомости, персональные учетные данные и данные о деловых операциях. Потеря хотя бы одного сегмента этой информации, даже на короткое время, препятствует нормальной работе организации. Представьте себе, что из системы исчезла информация, касающаяся оплаты труда работников, и все или часть работников не получили во время зарплату. Мы бы не хотели присутствовать при этом!

Случаи потери данных могут быть легкими, как, например, при порче одного файла, или тяжелыми, как при утрате возможности чтения всего содержимого жесткого диска сервера. Организации могут почти полностью избежать проблем, связанных с потерей данных, за счет регулярного резервирования данных, которые хранятся в ее компьютерных сетях.

Все типы угроз представляют собой опасность для данных. Все, от пожара до компьютерных вирусов, может уничтожить данные в сети. Составление планов в отношении каждого типа чрезвычайных ситуаций может помочь вам, случись беда, полностью сохранить и восстановить данные вашей организации.

Потеря данных в сети может произойти по разным причинам. Если вы знаете, в чем состоит потенциальная угроза, и готовитесь к ней, вы можете предотвратить как серьезное повреждение сети, так и потерю данных. Мы настоятельно советуем вам всегда создавать резервную копию сетевых данных и поочередно сменять последнюю копию вне системы.

Ниже приведен перечень некоторых потенциальных угроз, которым может подвергнуться ваша сеть.

- ✓ Аварийный отказ жесткого диска. Даже если ваш сервер оснащен встроенной системой обеспечения отказоустойчивости (наподобие зеркальных или спаренных дисков), не следует рассчитывать на то, что эти методы всегда работают и позволяют добиться восстановления всех данных на 100 процентов. Мы видели зеркальные диски, которые незаметно выходили из синхронного режима, что удавалось обнаружить только после отказа жесткого диска. При отсутствии резервной копии вы можете потерять все данные или их сегменты. Зеркальное или спаренное дублирование неплохо дополнять регулярным резервированием.
- ✓ Резкое отключение. Время от времени вы сталкиваетесь с самоуверенным работником, который резко ударяет по выключателю сервера, что приводит к его некорректному отключению. Большинство серверов сегодня нормально восстанавливает предшествующее состояние — но не всегда. Отключение сервера подобным образом может привести к тому, что жесткий диск станет нечитаемым. Вы должны поместить серверы в надежное место вдали от конечных пользователей. И не забывайте о регулярном резервировании!
- ✓ Вирусы. Многие организации, подключенные к Internet, позволяют работникам загружать в локальную сеть любые типы данных, которые могут внести вирусы. Вирусы несут реальную угрозу организации. Один вирус может разрушить весь компьютер и сделать его непригодным в очень короткое время. Если этому компьютеру случится быть сервером в сети, некто начнет читать секретную информацию ваших работников. Установка антивирусного ПО на сервере позволит проверить наличие вирусов прежде, чем они будут запомнены на сервере. Составьте план, который позволит вам восстановить данные в сети в том виде, в котором они были до занесения вируса.
- ✓ Природные катастрофы. Мы знаем немало организаций, которые потеряли данные во время природных катаклизмов, например сильного шторма, Если молния может вывести из строя электронику у вас дома, представьте, что она может сотворить с данными в вашей сети.

  Вот некоторые природные бедствия, к которым вы должны быть готовы.

  - Пожар. Один пожар в здании или на этаже может уничтожить целую организацию. Если ваша организация потеряет в пожаре все, вы можете оказаться спасителем, если создадите копию текущих сетевых данных на магнитной ленте, которая лежит где-нибудь в безопасном месте. Но если вы храните кассеты с резервными копиями в машинном зале, вы будете одним из тех, кто окажется на улице.
  - Наводнения. Размещать машинный зал, сервер или резервное оборудование в подвале или на первом этаже здания — плохая идея, в особенности в местности, подверженной наводнениям. Одно наводнение может стереть с лица земли целую организацию. Даже если наводнение произойдет, ваши кассеты с резервными копиями вне офиса будут в безопасности — вдали от зоны наводнения.

- Ураганы. Ураганы несут с собой страшные ветры и дождь. Не помещайте сервер или резервное оборудование в машинном зале с открытыми окнами. Вы можете вернуться и обнаружить, что все разбросано по машинному залу и насквозь промокло, — и у вас нет кассеты с резервной копией для восстановления.
- Повышенная температура. Такая простая вещь, как размещение сервера или резервной машины в закрытой комнате без надлежащего кондиционирования и вентиляции, может стать причиной проблем. Не помещайте сервер или резервное оборудование в небольшой комнате вместе с другим выделяющим много тепла оборудованием, например с копировальным аппаратом, не обеспечив воздушный поток через нее. Вентиляционные системы зданий отключаются на выходные и по праздникам, и тепло может погубить сервер.

Некоторые вирусы обладают "инкубационным" периодом; поэтому они могут быть занесены в вашу сеть, но не замечены в течение нескольких дней. Мы видели рассерженных работников, которые внесли вирусы в сеть, а затем покинули компанию — 30 дней спустя вирус проявился. Учтите это обстоятельство в вашем плане за счет постоянного резервного копирования по 30-дневной схеме чередования копий. Если вирус наподобие этого проник в вашу сеть, вы можете вернуться как минимум к своим резервным лентам 30-дневной давности, чтобы попробовать восстановить сетевые данные в том состоянии, в котором они находились до появления вируса. Если в вашем распоряжении только недельные копии, все они содержат вирус. Антивирусное ПО от компаний Norton (www.symantec.com) и McAfee (www.mcafee.com) склонно к конфликтам с Windows Server 2003 меньше, чем любые другие марки антивирусного ПО.

Типы резервирования

В мире компьютеров существует всего пять типов резервирования данных, и то же самое справедливо в отношении возможностей Windows Server 2003. Ниже перечислены пять типов резервирования, имеющихся в системе Windows Server 2003.

- ✓ Нормальное резервирование.
- ✓ Резервирование копированием.
- ✓ Ежедневное резервирование.
- ✓ Дифференциальное резервирование.
- ✓ Добавочное копирование.

Прежде чем вы сможете действительно понять эти методы, вы должны знать, что такое *бит архива (archive bit)*. Файлы обладают атрибутами, которые есть не что иное, как свойства файла. Один из атрибутов, присутствующих в системах Windows 2003, представляет собой бит архива. После создания или модификации файла его бит архива автоматически сбрасывается операционной системой. Бит архива указывает, что файл необходимо резервировать, даже если ПО резервирования не установлено или не сконфигурировано на компьютере. Программное обеспечение резервирования проверяет этот бит, чтобы определить состояние файлов. Вы можете представлять его себе как пломбу на каждом из файлов вашей системы. Когда операционная система, пользователь или приложение модифицируют файл, пломба срывается. После этого ПО резервирования испытывает файл и заново "пломбирует" его, создавая для него резервную копию.

Нормальное резервирование

Нормальное резервирование (normal backup) состоит в копировании всех выбранных файлов и установлении бита архива, который указывает ПО резервирования на то, что для файлов создана резервная копия. Этот тип резервирования применяется при первом резервировании данных компьютера. Также при этом виде резервирования для восстановления всех файлов требуется только последняя кассета. (Резервирование с использованием кассет более подробно рассматривается ниже, в разделе "Локальное резервирование".)

Резервирование копированием

Резервирование копированием (copy backup) полезно, поскольку оно не устанавливает бит архива и, следовательно, не влияет на нормальное или добавочное копирование. Его можно использовать для копирования выбранных файлов в промежутках между запланированным нормальным или добавочным резервированием. (Добавочное резервирование более подробно рассматривается ниже, в разделе "Добавочное резервирование".)

Ежедневное резервирование

При *ежедневном резервировании (daily backup)* копируются те выбранные файлы, которые были изменены в день, когда стартовало задание на резервирование. Ежедневное резервирование не устанавливает бит архива. Этот вид резервирования можно использовать для копирования только тех файлов, которые были изменены в этот день, и поскольку бит архива не устанавливается, регулярное резервирование идет своим чередом.

Дифференциальное резервирование

Подобно резервированию копированием и ежедневному копированию, *дифференциальное резервирование (differential backup)* также не устанавливает бит архива. Оно копирует все файлы, которые были созданы или модифицированы с момента последнего нормального или добавочного резервирования. Один из приемов заключается в том, чтобы использовать сочетание обычного и дифференциального резервирования для настройки конфигурации задания на резервирование для компьютера. При таком сочетании нормальное резервирование выполняется еженедельно, а дифференциальное — ежедневно. При использовании подобного задания на резервирование и проведение восстановления требуются только ленты с последней обычной или дифференциальной копией.

Добавочное резервирование

Добавочное резервирование (incremental backup) похоже на дифференциальное тем, что оно резервирует только те файлы, которые были созданы или модифицированы с момента последнего нормального или добавочного резервирования. Но в отличие от дифференциального резервирования добавочное резервирование устанавливает бит архива, который указывает, что файлы подвергнуты резервированию. Сочетание обычного и добавочного резервирования можно использовать для настройки конфигурации задания на резервирование. При таком сочетании нормальное резервирование используется еженедельно, а добавочное — ежедневно. Чтобы восстановить файлы, для которых использовался этот вид резервирования, требуются последние обычный и все добавочные наборы.

Настройка конфигурации задания на резервирование для использования этого сочетания не занимает много времени и позволяет сэкономить память, поскольку резервируются только те файлы, которые подверглись модификации. Однако важно иметь в виду, что восстановление данных в этом случае значительно труднее и занимает больше времени по сравнению с комбинацией дифференциального и нормального резервирования, поскольку вы должны использовать полный набор дополнительных кассет. Этот вид комбинации или конфигурации

резервирования представляет собой идеальный вариант для предприятий, где можно использовать автоматизированную библиотеку (магнитных) лент (automated tape library — ATL). При использовании ATL ПО резервирования контролирует все операции по восстановлению данных, включая решение о загрузке правильной последовательности кассет с использованием ее “ механической руки".

В основе библиотеки ATL лежит программно-управляемая система, в которой нет необходимости в загрузке и смене лент. Типичная система ATL обычно построена вокруг контейнера/библиотеки, которая может содержать от нескольких лент до нескольких сотен лент, при этом каждая лента идентифицируется уникальным штрих-кодом. Внутри библиотеки находится от одного до нескольких лентопротяжных устройств для чтения и записи лент, Система ATL также включает механизм, отвечающий за установку ленты (кассеты) на лентопротяжное устройство и снятие ее с устройства. Этот механизм может представлять собой "механическую руку" (в случае больших ATL-систем) либо простую систему наподобие тех, которые используются в кассетном магнитофоне. ПО резервирования управляет всеми операциями, давая инструкции "механической руке" по загрузке определенной ленты в определенное лентопротяжное устройство и заданию на резервирование или восстановление.

Сеть или локальное резервирование

При резервировании сетевой информации вы можете выбирать между сетевым и локальным резервированием. В этом разделе мы рассматриваем особенности каждой из возможностей.

Сетевое резервирование

Сетевое резервирование используется в крупномасштабных сетевых средах. При использовании сетевого резервирования конфигурация хост-компьютера настраивается таким образом, чтобы резервировать данные удаленных компьютеров, подключенных к хост-компьютеру через локальную сеть. В этом сценарии данные перемешаются от удаленного компьютера по сети к хост-компьютеру, в конфигурацию которого входит лентопротяжное устройство. После выгрузки данных из сетевого интерфейса (адаптера) в шину компьютера данные трактуются в качестве локальной резервной копии. (Информация о том, как настроить конфигурацию сервера для резервирования данных удаленного компьютера, приведена ниже, в разделе "Возможности резервирования Windows Server 2003”.)

Данный тип резервирования может быть связан с проблемой скорости обмена, поскольку прохождение данных через локальную сеть создает регулярный трафик. При этом более чем желательно, чтобы локальная сеть была спроектирована под 10- или 100-мегабитовую технологию Ethernet. В противном случае скорость передачи данных в сравнении с локальным резервированием сильно падает. Чтобы справиться с проблемой и удовлетворить нужды предприятия, где каждую ночь требуется резервировать большие объемы данных, в отрасли была разработана архитектура “сервер–хранилище данных" (Storage Area Network — SAN). В этой архитектуре все компьютеры и устройства хранения данных подключены непосредственно к ответвлению волоконно-оптического канала с арбитражной логикой Fiber Channel Arbitrated Loop (FC-AL), пропускная способность которого составляет около 100 Мбит/с. Более того, эту пропускную способность используют только компьютеры и устройства резервирования. Подобная архитектура дорогостояща, однако она многократно окупает свою высокую стоимость.

Локальное резервирование

Конфигурация системы локального резервирования состоит из локального лентопротяжного устройства, подключенного к компьютеру или установленному на нем с помощью интерфейсов ШЕ (Integrated Device Electronics — встроенный интерфейс устройств) или SCSI (Small Computer Systems Interface — интерфейс малых компьютерных систем). Локальное резервирование работает быстро, поскольку, когда вы используете эти интерфейсы, ленто-

протяжное устройство подключено непосредственно **к шине** компьютера. Для некоторых новых SCSI-интерфейсов, таких как Ultra2 Wide SCSI, скорость передачи может достигать 80 Мбит/с. Скорее всего, подобная скорость недостижима, так как лентопротяжное устройство может обеспечить скорость от 4 до 10 Мбит/с в зависимости от типа устройства. Благодаря современным достижениям в области аппаратного обеспечения для подобной системы возможно получить производительность около 15 Гбит в час.

Локальное резервирование относительно недорого, поскольку в его стоимость входят только стоимость лентопротяжного устройства, магнитных лент (кассет) и, по необходимости, ГОЕ- или SCSI-интерфейса. Большинство компьютеров оснащено дополнительным ГОЕ- или SCSI-интерфейсом, который можно использовать для этой цели. Если требуется ПО резервирования от независимого поставщика, то в стоимость дополнительно включается стоимость лицензии на это ПО. Однако Windows Server 2003 поставляется с мощным ПО резервирования, которое является бесплатным!

Резервные ленты, которые мы используем (Hewlett Packard DDS 3), вмещают до 24 Гбайт данных. В зависимости от того, какой объем данных вам необходимо резервировать и какой тип кассеты вы используете, вам может потребоваться больше одной кассеты для хранения всех данных.

Знакомство с технологией

Независимо от того, выбираете ли вы сетевое или локальное резервирование, и независимо от частоты, с какой вы решили выполнять резервирование, вам необходимо освоить некоторую терминологию и технологию, которые касаются оборудования, используемого в системах резервирования, и различные методы резервирования.

Оперативное, полуавтономное, автономное

Вы наверняка слышали о возможностях оперативного, полуавтономного и автономного хранения данных. Выберите метод, который подходит вашей организации по затратам времени и усилий, в зависимости от того, насколько часто вы восстанавливаете ваши данные и насколько быстрый доступ к ним вам требуется. Ниже приводится описание этих типов резервирования.

- **Оперативное (Online).** Этот вид резервирования обычно осуществляется на сервере, как правило, в форме второго жесткого диска — зеркального или дублирующего. Пользователи без труда могут получить доступ к данным посредством их настольных систем без вашего вмешательства, за исключением того, что вы должны регулярно проверять уровень отказоустойчивости системы. Синхронизация устройств может незаметно нарушиться, если вы не следите за устройствами вручную или с помощью программы.
- **Полуавтономное (Nearline).** Это резервирование осуществляется на устройстве, подключенном к сети. Полуавтономное резервирование требует некоторого вмешательства с вашей стороны, поскольку оно обычно использует некоторый неизвестный для пользователя метод, такой как метод упаковки данных. Данные находятся под рукой, но ваши пользователи не знают, как выполнять функции наподобие распаковки файлов, чтобы получить доступ к данным.
- **Автономное (Offline).** Этот тип резервирования охватывает устройства, которые работают под управлением собственного ПО и отделены от сервера. Вам необходимо знать, как работать с этими устройствами, поскольку пользователи могут не знать способа доступа к данным или не обладать правами доступа к ним. Эти устройства, как правило, самые медленные, так как данные должны перемещаться с сервера на другое устройство. Многие организации размещают эти устройства в сетевой магистрали и подключаются к ним через оптоволоконный кабель для повышения скорости передачи данных.

Второй и третий способы резервного копирования более дорогостоящие, требуют больше времени на доступ к информации и большего вмешательства с вашей стороны.

Используемое оборудование

Системы резервирования состоят из устройств резервирования, среды резервирования и программных компонентов. В зависимости от ваших потребностей вы можете использовать системы самого разного масштаба, вида и стоимости. В этом разделе мы описываем наиболее распространенные системы, так что вы сможете обсудить с вашим поставщиком проблемы удовлетворения своих сетевых потребностей.

Устройства резервирования

Устройство резервирования (backup unit) — это оборудование, которое может быть простым, как, например, лентопротяжное устройство с одним гнездом, или сложным, как, например, проигрывающая система со сменой дисков с помощью "механической руки". Если ваши требования к памяти для данных невелики, вполне достаточно простого лентопротяжного устройства резервирования с большей емкостью, чем у вашего сервера. Подобные устройства не так дороги и имеются в наличии в компьютерных магазинах. Некоторые из этих устройств имеют шлейфовую организацию и не требуют вашего присутствия для смены кассет.

Если вашей организации необходимо резервировать большие объемы данных, вы должны рассмотреть подход на основе *"вертушки"* (*jukebox*). "Вертушка" — это устройство, похожее на небольшой компьютерный вертикальный блок с дверцей. Внутри размещаются несколько гнезд, а также "механическая рука", которая может вставлять и передвигать кассеты или компакт-диски. При использовании этого типа системы вы обычно можете вставить недельный запас резервных кассет и позволить системе автоматически выполнять резервирование.

Еще одним видом устройств резервирования являются *магнитооптические диски (magneto-optical drives),* которые сочетают в себе технологию магнитной и оптической записи, позволяющей создавать перезаписываемые резервные копии данных. Преимущество этой технологии заключается в том, что она обеспечивает произвольный доступ к данным — более быстрый, чем последовательный. Устройства этого типа недороги, но носители резервных копий существенно дороже. Если вам требуются большие объемы данных и быстрый доступ к ним, обратите внимание на эту технологию.

Каждый тип устройств резервирования оснащен некоторым видом гнезда, куда помещается носитель. Размер этого гнезда зависит от устройства. Некоторые устройства оснащаются гнездами размером 4 и 8 мм, 1/4 и 1/2 дюйма и больше. Покупайте средства хранения, соответствующие размерам устройства хранения, поскольку вы не сможете вставить ленту размером 1/2 дюйма в устройство с гнездом размером 1/4 дюйма!

Носители резервных копий

Носители резервных копий (backup media) — это магнитные ленты, картриджи, CD-WORM (CD-Write-Once-Read-Many — компакт-диск с однократной записью и многократным считыванием), компакт-диски со стиранием информации (или перезаписываемые компакт-диски), дискеты и другие средства хранения данных. Любое приспособление, на котором устройство резервирования хранит данные, становится носителем. Существуют разные по форме, размерам и толщине носители резервных копий. Вы должны убедиться в том, что следуете указаниям производителя по приобретению носителей для своего устройства.

Не покупайте для резервирования картриджи с видеолентами в магазине, торгующем со скидками. Приобретайте магнитные ленты для хранения данных, которые стоят дороже, но предназначены для более жесткой эксплуатации.

Носители резервных копий поставляются не только разных физических размеров, но также и разной емкости. Некоторые магнитные ленты хранят до 24 Гбайт данных. Перезаписы-

ваемые компакт-диски хранят до 650 Мбайт неупакованных данных и гигабайты данных в упакованном виде. Независимо от выбранного устройства и носителя всегда приобретайте их в избытке, чтобы вы могли чередовать их, не используя постоянно один и тот же носитель. Мы видели ребят, которые покупали всего одну ленту и использовали ее снова и снова, пока не приходило время восстановления данных. Легко догадаться, что в итоге лента оказалась сбойной; поэтому ребята оказались без резервной копии! Распределите резервные копии по нескольким лентам, чтобы минимизировать риск потери резервных данных. Как говорится, не кладите все яйца в одну "ленточную" корзину!

Программное ***обеспечение***

Вы можете использовать встроенное ПО резервирования Windows Server 2003 на устройствах резервирования независимых поставщиков либо использовать ПО, которое поставляется с этими устройствами. Мы предпочитаем использовать ПО независимых поставщиков, поскольку оно предназначено для работы с определенными промышленными устройствами и для них всегда имеются в наличии соответствующие драйверы. Установка устройств пройдет более гладко, если вы будете использовать рекомендуемое ПО. Всегда держите копию ПО резервирования вне офиса на случай пожара или другого бедствия. Если вы потеряли все оборудование, вам необходимо перезагрузить это ПО на другую машину прежде, чем вы сможете восстановить данные.

Великолепные возможности утилиты NTBACKUP Windows Server 2003

Более всего программа NTBACKUP Windows NT Server разочаровывает тем, что она может резервировать данные только на лентопротяжном устройстве. Нет ничего необычного в том, что у вас может возникнуть необходимость получить резервную копию информации, содержащейся в системе с лентопротяжным устройством, и восстановить ее в системе, в которой лентопротяжное устройство отсутствует. Программа NTBACKUP Windows Server 2003 позволяет создавать резервные копии на любом приемлемом для вас носителе, включая флоппи-диски, ZIP-накопители, JAZ-устройства, сетевые диски на сервере или вторые жесткие диски.

- Служба управления съемными устройствами хранения (Removable Storage Manager— RSM) является неотъемлемой частью операционной системы Windows 2003. Эта служба отвечает за управление задачами наподобие монтирования или демонтажа устройств хранения со стороны ПО резервирования Windows 2003. Замена ПО резервирования для выполнения этих задач и придание им статуса части операционной системы, в отличие от предыдущих версий Windows NT, позволила повысить надежность и устойчивость этого ПО.
- Одно из наиболее поразительных свойств утилиты резервирования Windows 2003 известно как автоматическое восстановление системы (Automated System Recovery— ASR). ASR представляет собой функцию, которая позволяет восстановить важные системные файлы в случае их повреждения, удаления или других отказов системы. ASR не сохраняет параметры установленного приложения или какие-либо личные данные. Она сохраняет только файлы, необходимые для загрузки и запуска ОС. Набор носителей ASR представляет собой загрузочную дискету и одну или несколько резервных магнитных лент. Для восстановления системы с использованием ASR вам необходимо загрузить с исходного дистрибутивного компакт-диска для Windows Server 2003 и нажать клавишу <F2> в ответ на приглашение инициировать процесс восстановления ASR.
- Наконец, вы можете осуществить резервирование (и восстановление) с помощью, мастера резервирования (Backup Wizard). Мастер задаст вам вопросы, на которые вы должны ответить для корректного выполнения резервирования. Более подробно мастер резервирования рассматривается ниже, в разделе "Планирование заданий на резервирование".

Планирование резервирования

Одна из наиболее важных задач, которая стоит перед вами, — планирование операций резервирования. Некоторые из лучших систем и методов резервирования все еще могут оказаться неадекватными, поэтому разумно проверить их эффективность в первую очередь.

Храните ленты с резервными копиями вне офиса

Нет ничего необычного в том, что компании хранят свои резервные ленты в несгораемых шкафах, обычно расположенных в машинном зале, где может возникнуть пожар. Подобная безопасность хороша только для бумаги. Эти шкафы выдерживают достаточно высокую температуру, поэтому бумага не сгорает. Однако этого тепла более чем достаточно, чтобы расплавить любую ленту, которая может в них храниться. По этой причине более толковые компании хранят свои ленты вне офиса, обновляя резервные копии ежедневно, еженедельно или ежемесячно (в зависимости от частоты изменения данных). Хранение данных вне офиса обеспечивает сохранность данных в случае такого бедствия, как пожар или наводнение.

Существуют компании, которые хранят данные вне офиса за плату. Магнитные ленты периодически отбираются и передаются в стороннее помещение для хранения. По необходимости потребители могут запросить доставить необходимые ленты для восстановления. Подобные компании могут заключать различные контакты на обслуживание. Хотя подобное обслуживание 24 часа в сутки 7 дней в неделю обходится недешево, дополнительные затраты на обеспечение готовности лент могут быть оправданы в зависимости от вида деятельности компании и важности данных.

Документально фиксируйте оборудование и его параметры

Особенно важно документально зафиксировать оборудование и его параметры, поскольку это экономит время, которое приходится тратить на оценивание и испытание различных конфигураций, связанных с получением системных резервных копий и последующим восстановлением данных с ленты. Следует фиксировать все важные параметры, такие как обьемы томов или дисков, используемые файловые системы и их тип — FAT (File Allocation Table — таблица размещения файлов) или NTFS (New Technology File System — файловая система Windows NT). Если вы используете в дисковой подсистеме некоторый вид отказоустойчивости, например зеркальный диск или RAID-систему (Redundant Array of Inexpensive Devices — матрица недорогих устройств с избыточностью), необходимо зафиксировать эти подробности. В общем, аккуратное и исчерпывающее документирование служит гарантией быстрого и надежного восстановления.

Вы также должны составить перечень номеров частей всех компонентов, установленных в вашей системе. Также включите список всех поставщиков и свою контактную информацию. Если компоненты вашей системы поставляются одним из крупных изготовителей серверов, таких как Compaq или Hewlett Packard, они могут дать вам систему для восстановления ваших данных. Наконец, всегда держите наготове драйверы всех устройств.

Применяйте аварийное восстановление для системы

Целесообразно периодически применять аварийное восстановление, чтобы убедиться в его действенности в случае, если оно потребуется после реального бедствия. В крупных компаниях это обычная практика, фактически предписываемая руководством. Несмотря на легкость подобного утверждения, реально внедрить эту практику значительно труднее, чем вы можете себе представить. Проблема заключается в том, что вы можете попытаться восстановить ваши данные в производственной системе (которая представляет собой систему, предна-

значенную для выполнения другой функции). Если вы поступите таким образом и резервная копия разрушена, ваши реальные данные также станут недостоверными. Многие организации в качестве резервной приобретают вторую систему с такой же спецификацией, что и производственная система. Эти системы обычно "заимствуются" из других пилотных проектов и внедряются в производство.

Windows Server 2003 обладает новыми возможностями, которые значительно облегчают аварийное восстановление. Эти возможности аналогичны решениям независимых поставщиков, в которых восстановление всей системы возможно с помощью нескольких дискет. Более подробную информацию об аварийном восстановлении можно получить в справочной системе и центре поддержки (Support Center) Windows 2003.

Возможности резервирования Windows 2003

Компания Microsoft уже включала программу резервирования под названием NTBACKUP в операционную систему Windows NT. Windows 2003 продолжает эту традицию. Версия утилиты NTBACKUP для Windows Server 2003 сохранила способность создавать резервные копии на носителях, отличных от магнитной ленты, и осуществлять доступ к сетевым ресурсам; кроме того, она включает встроенные возможности планирования. Эти возможности были представлены в версии этого средства для Windows 2000, но отсутствовали в версии для Windows NT.

Общая картина

Windows Server 2003 поставляется с новой версией программы NTBACKUP, которая включает два метода резервирования данных сервера: с помощью GUI-интерфейса (Start⇨All Programs⇨Accessories⇨System Tools⇨Backup (Пуск⇨Программы⇨Стандартные⇨Служебные⇨Архивация данных)) и запуска программы из командной строки (\WINNT\system32\ntbackup). Мы предпочитаем усовершенствованное средство на основе GUI-интерфейса (рис. 17.1) для быстрого создания резервной копии вручную и интерфейс командной строки для пакетного и планового резервирования.

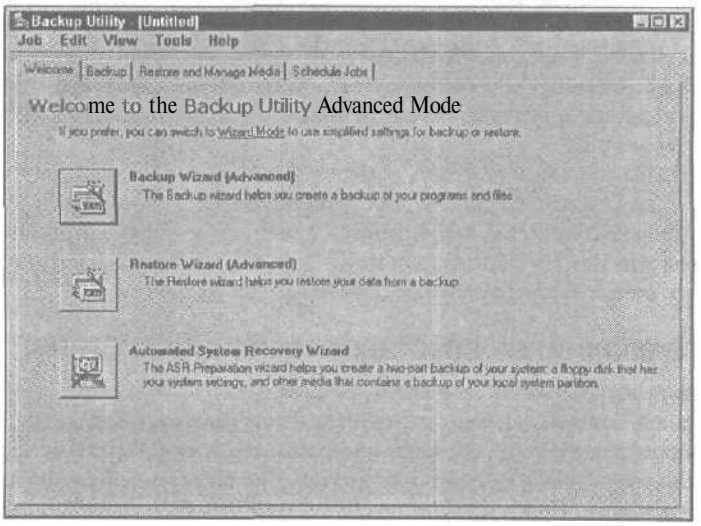


Рис. 17.1. Встроенная GUI-утилита резервирования Windows 2003

Эти методы не являются полностью автоматическими, поскольку вы должны запустить их вручную, — если только вы не установили их автоматический запуск в текущий момент с помощью задачи планировщика. Хотя все выглядит несколько топорно и не так, как хотелось бы, все же программа NTBACKUP лучше, чем ничего. Если ваш бюджет ограничен и вы не можете позволить себе приобрести решение от независимого поставщика, который специализируется на ПО резервирования, — это выход из положения. И самое приятное, что эта программа — бесплатная (точнее говоря, ее стоимость включена в цену Windows Server 2003)!

Прежде чем покупать продукт резервирования от независимого поставщика или использовать встроенную программу Windows Server 2003, обратитесь к базе знаний компании Microsoft (www.microsoft.com/support/), чтобы узнать о дефектах и проблемах, связанных с вопросами резервирования. В своем поиске в базе знаний будьте точны (т.е. квалификация поиска должна выглядеть как Windows Server **NTBACKUP).** Также всегда устанавливайте последний служебный пакет, который долен исправлять наиболее неприятные дефекты, известные Microsoft.

Запуск утилиты резервирования из командной строки

Для запуска программы NTBACKUP из командной строки используется следующий синтаксис:

```
ntbackup backup [systemstate] "@bks file name" .
/J {"job name"} [/P {"pool name"}] [/G {"guid name"}]
[/T {"tape name"}] [/N{"media name"}] [/F {"file name"}]
[/D {"set description"}] [/DS {"server name"}]
[/IS {"server name"}] [/A] [/V:{yes|no}] [/R:{yes|no}] .
[/L:{f|s|n}] [/M {backup type}] [/RS:{yes|no}]
[/HC:{on|off}] [/SNAP:{on|off}] . .
```

Выглядит чересчур сложно! Однако не следует волноваться, все не так плохо. В большинстве случаев вам потребуется только часть параметров, а не все. Лучше всего узнать подробности, касающиеся запуска программы NTBACKUP, в руководстве Command-line Reference, доступ к которому осуществляется с помощью команды **ntbackup/?**, введенной в поле команды Run (Выполнить). В результате отобразится окно справки, содержащее правильный синтаксис для NTBACKUP, вместе с отличными описаниями, ограничениями, требованиями и советами по использованию каждого параметра. Кроме того, несколько примеров помогут вам разобраться с тем, как использовать синтаксис командной строки.

Однако в действительности мы не видим особой нужды в работе с программой NTBACKUP посредством командной строки, особенно если учесть, что GUI-средства обеспечивают резервирование по расписанию.

Некоторые файлы, которые жестко запрограммированы в NTBACKUP, не поддаются резервированию, и вы не сможете ни изменить, ни переделать программу. Ниже приведен перечень некоторых файлов и других объектов, которые не подлежат резервированию.

- ✓ Открытые файлы. В процессе резервирования не может быть открытых файлов. Такие файлы не резервируются Пользователи должны выйти из системы и отключить ее от совместно используемых ресурсов.
- ✓ Временные файлы. Временные файлы наподобие PAGEFILE.SYS не резервируются.
- ✓ Разрешения. Учетные записи, используемые для выполнения резервирования, должны иметь разрешение на чтение файлов.
- ✓ Реестр. Резервируется только локальный реестр. Реестры других серверов не резервируются.

Выбор файлов и папок

В версии NTBACKUP для Windows NT вы могли выбрать файлы, которые намерены резервировать, только посредством GUI-интерфейса. Версии программы для Windows 2000 и 2003 позволяют вам либо выбрать корневой диск или каталог в командной строке, либо использовать GUI-интерфейс для определения файлов, выбираемых для резервирования (файлы с расширением .bks). Чтобы создать bks-файл, выполните следующие действия.

1. **Выберите команду Start⇨All Programs⇨Accessories⇨System Tools⇨Backup.**
   Появится окно приглашения мастера резервирования и восстановления.
2. **Щелкните на кнопке Advanced Mode (Расширенный режим).**
3. **Щелкните на вкладке Backup (Архивация).**
4. **Выберите требуемые папки и диски, которые вы намерены резервировать (рис.** 17.2).
5. **Выберите команду Job⇨Save Selection (Задание⇨Сохранить выбор).**
6. **Выберите имя для .bks-файла.**
7. **Используйте параметр имени bks-файла как часть синтаксиса командной строки.**

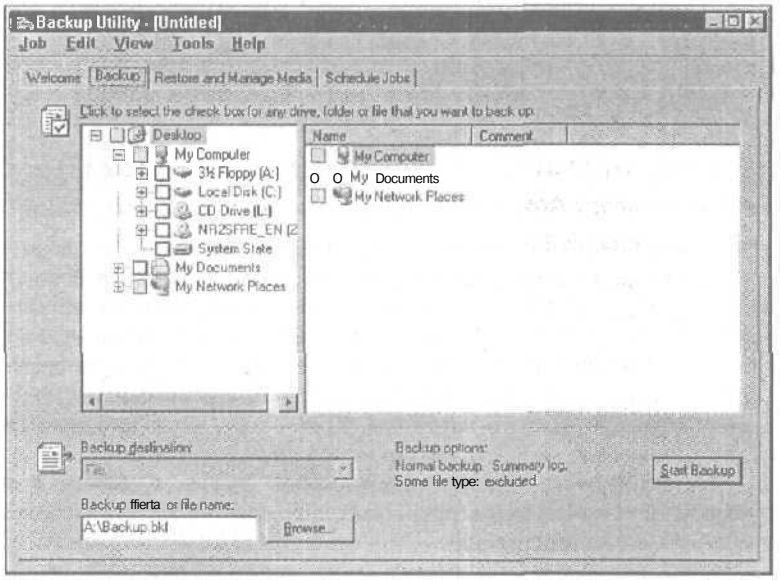


Рис. 17.2. Выбор файлов и папок, подлежащих резервированию

Если вы предпочитаете использовать GUI-версию программы NTBACKUP, пропустите п. 7 и прочтите следующий раздел "Определение места записи резервной копии и параметров носителя", который содержит подробности об использовании GUI-версии.

Определение места записи резервной копии и параметров носителя

Теперь, когда вы выбрали файлы, которые намерены резервировать, можете выбрать место записи резервной копии- Если в вашей системе не установлено лентопротяжное устройство, программа NTBACKUP по умолчанию выберет в качестве места записи резервной копии

файл. Или же выберите резервное устройство, на которое вы желали бы скопировать информацию, следующим образом.

1. **Выберите команду Start⇨All Programs⇨Accessories⇨System Tools⇨Backup.**

   Появится экран приглашения мастера резервирования и восстановления.

2. **Щелкните на кнопке Advanced Mode (Расширенный режим).**
3. **Щелкните на вкладке Backup (Архивация).**
4. **Выберите местоположение копии (файл или ленту).**
   - Если вы выбираете копирование данных в файл, выберите пункт File (Файл) в выпадающем списке Backup Destination (Место назначение архива). Введите в поле Backup Media or File Name (Носитель архива или имя файла) полный путь и имя файла (или щелкните на кнопке Browse (Просмотр), чтобы определить его).
   - Если вы выбираете копирование данных на ленту, выберите ленту из выпадающего списка Backup Destination.
5. **Щелкните на кнопке Start Backup (Архивировать).**

Планирование заданий на резервирование

Как упоминалось ранее, планирование заданий на резервирование стало теперь встроенной функцией Windows Server 2003. Планирование заданий на резервирование можно выполнить с помощью следующих действий.

1. **Выберите команду Start⇨All Programs⇨Accessories⇨System Tools⇨Backup.**
2. **Щелкните на кнопке Advanced Mode (Расширенный режим).**
3. **Щелкните на вкладке Backup (Архивация).**
4. **Щелкните на кнопке Add Job (Добавить задание).**

   Запустится мастер-программа резервирования,

5. **Ответьте на вопросы, которые вам задаст мастер.**

   Обратите внимание, что вы получите запрос указать имя пользователя и пароль. Пользователь, выполняющий резервирование (возможно, вы), должен быть либо администратором, либо членом группы операторов резервирования (Backup Operators), либо иметь права, равные с членами этих групп.

6. **Задайте частоту выполнения задания и щелкните на кнопке Finish (Готово).**

Календарь во вкладке Schedule Job (Запланированные задания) изменится, отображая расписание заданий.

Восстановление данных из резервной копии

Резервирование данных составляет только половину дела. Вторая половина охватывает восстановление файлов в сети. Мы надеемся, что вам приходится восстанавливать время от времени только несколько файлов для пользователей. Постоянное создание регулярных резервных копий делает эту задачу простой и приятной. Однако при пожаре или другом бедствии вы можете утратить данные и компьютерное оборудование, включая сервер, на котором вам необходимо восстановить данные. Мы надеемся, что вы последуете нашему совету о еженедельном чередовании хранимых вне офиса магнитных лент, чтобы подготовиться к подобного рода катастрофе. Если вы также потеряли сервер, мы надеемся, что у вас хорошие

рабочие отношения с поставщиком, так что **вы** сможете без промедления получить необходимое оборудование.

Самое важное, что следует помнить при восстановлении данных сети, — это о необходимости практиковаться в процессе восстановления, пока "гром не грянул". Это не только даст вам возможность приобрести опыт в выполнении этой задачи, но и позволит периодически проверить целостность резервной копии. Хотя вы можете каждое утро проверять файл журнала, лучше выполнять реальные испытания восстановления — нечто вроде генеральной репетиции. Когда придет беда и вам потребуется выполнить реальное восстановление, все, кому не лень, станут заглядывать вам через плечо и приставать с вопросом: "Когда же все заработает?" Если вы хорошо знаете свою систему резервирования, вы сможете выполнить эту задачу в крайне тяжелых условиях. Не дожидайтесь последней минуты, чтобы испытать и изучить систему.

Сначала всегда восстанавливайте системные файлы (\SYSTEM32\CONFIG и файлы реестра), перезагрузитесь, а затем бросьте взгляд на систему, чтобы убедиться, что все на месте. Затем восстанавливайте файлы данных. Если структура каталога и тома предусматривает сегментирование системы и файлов данных, эта задача намного легче. Продумайте наперед, данные каких подразделений должны восстанавливаться в первую очередь. Иногда в этом нет необходимости, но в некоторых случаях при наличии подразделений по обслуживанию клиентов требуется, чтобы сеть была возвращена в исходное состояние как только будет обеспечен доступ к их данным. Почему? Потому что они обслуживают внешних клиентов, которые приносят прибыль вашей организации! Прежде чем возникнет необходимость в восстановлении данных, попробуйте составить план порядка восстановления и испытать его на практике.

Учтите, что иногда вы не сможете восстановить системные файлы Windows 2003; вы можете переустановить Windows 2003, а затем восстановить системные файлы.

Средства резервирования данных, предлагаемые независимыми разработчиками

Поскольку Windows 2003 — совершенно новая операционная система, сегодня для нее не существует специальных возможностей, предлагаемых независимыми разработчиками. Однако можно быть уверенными в том, что подобная ситуация не продлится долго.

Мы всегда советуем иметь дело с известными, заслужившими доверие независимыми компаниями, чтобы обеспечить совместимость с Windows Server 2003 и другими сетевыми операционными системами. Большинство известных пакетов поддерживает возможности одновременного резервирования нескольких различных операционных систем и обладает легким в использовании интерфейсом резервирования и восстановления.

Одним из простейших способов отыскать ПО резервирования от сторонних разработчиков — посетить один из популярных поисковых серверов сети, например `http//search.cnet.com/`, и ввести ключевую фразу **Windows Server 2003Backup**. Торгующие со скидкой Internet-магазины, наподобие CDW (`www.cdw.com/`), предоставляют информацию о различных устройствах резервирования в одном удобном месте. На Web-узле CDW войдите в раздел Hardware?. Щелкните на опции Data Storage и посмотрите, насколько исчерпывающую информацию вам предлагают.

На рынке ПО резервирования существуют поставщики двух типов: компании, которые предлагают решения по резервированию данных для малого бизнеса, и компании, которые предоставляют решения по резервированию данных в масштабе предприятия. Чтобы вы могли с чего-то начать свой поиск, мы перечислим наиболее известные компании-разработчики в каждой из этих групп.

- ✓ **Компании, предлагающие решения для малого бизнеса.**
  - Exabyte,www.exabyte. com;
  - ADIC (Advanced Digital Information Corporation), www.adic.com/adicHomePage.jsp;
  - Hewlett-Packard,www.hp.com/country/us/eng/proserv/storage. html.
- ✓ **Компании, предлагающие решения в масштабе предприятия.**
  - Veritas,www.veritas.com;
  - Legato,www.legato.com.

Ознакомьте на Web-узлах поставщиков ПО резервирования данных с официальными документами и документами, касающимися стоимости владения этими программными продуктами. Эта информация предоставляется бесплатно и содержит компиляцию многочисленных исследований. Вы можете использовать эту информацию, чтобы убедить руководство в справедливости ваших требований в отношении приобретения ПО резервирования.

Независимо от выбранного вами поставщика приведенный ниже контрольный перечень предоставит в ваше распоряжение полезные критерии для оценки систем резервирования на магнитных лентах. Определите требования для вашей организации и узнайте у поставщика, обладает ли его продукт необходимыми вам свойствами, и должны ли вы доплачивать за некоторые дополнительные модули.

- ✓ **Критические системные файлы.** Существенным свойством любой системы хранения данных на ленте, которую вы приобретаете, является ее способность резервировать системные файлы Windows Server 2003 — в частности, реестр и журнал событий, информацию о безопасности, учетные записи пользователей и списки управления доступом — в дополнение к фактическим данным.
- ✓ **Индексирование данных.** При резервировании больших объемов данных важно, чтобы в процессе восстановления вы имели возможность получить каталог содержимого ленты за одну-две минуты. Вы не должны ожидать 30 минут всякий раз, когда у вас возникает необходимость просмотреть содержимое конкретной ленты.
- ✓ **Кроссплатформенная поддержка.** Данные сетей, поддерживающих несколько платформ, например сети Novell, Microsoft и UNIX, легче резервировать, если одна система резервирования может поддерживать больше одной платформы.
- ✓ **Резервирование клиентских данных.** Некоторые пользователи отказываются хранить данные в сети. В этом случае обратите внимание на пакеты, автоматизирующие процесс резервирования клиентских рабочих станций по всей сети, с использованием вашей системы резервирования на основе магнитных лент. Некоторые известные системы включают такую возможность. Узнайте у поставщика, какие клиентские операционные системы они поддерживают (Macintosh, UNIX, Windows 98 или OS/2.).
- ✓ **Автоматическое функционирование.** Некоторые системы на лентах работают подобно "вертушке" и оснащены "механической рукой", которая вставляет и вынимает ленты. Эти системы дорогостоящи, однако если объемы резервируемых данных велики и вам неохота всю ночь вставлять ленты, обратите внимание на эту функцию.
- ✓ **Возможности планирования.** Если вы намерены выполнять добавочное и полное резервирование в разные дни, присмотритесь к системам, которые обладают гибкостью и позволяют автоматизировать функции планирования на ежедневной или еженедельной основе.

- ✓ **Открытые файлы.** Это файлы, которые находятся в использовании в процессе операции резервирования. Не все системы резервирования предусматривают резервирование открытых файлов, а некоторые прекращают работу, натолкнувшись на открытый файл. Большинство систем пропускает подобные файлы и записывает в журнал файла сообщение об исключительной ситуации. Весьма перспективно, если ваша система резервирования обрабатывает открытые файлы
- ✓ **Безопасность и шифрование.** Для более масштабных производственных сред запросите у поставщика, каким образом его система обрабатывает информацию, передаваемую по сети, такую как пароли, и информацию, касающуюся учетных записей.
- ✓ **Управление иерархической памятью.** Вам необходимо убедиться в том, что продукт поставщика поддерживает оперативное, полуавтономное и автономное хранение и может управлять сразу всеми тремя.
- ✓ **Объем хранилища данных.** Вам необходимо выяснить, какой объем данных вы можете поместить в архив системы (Мбайт или Гбайт), каковы размеры лент, используемых системой (4 мм, 8 мм, DLT и др.), а также упаковывает ли система данные.
- ✓ **Удаленное администрирование.** Удаленное слежение за состоянием и ходом резервирования — весьма полезное свойство.
- ✓ **Масштабируемость.** Выясните, является ли система масштабируемой и можно ли ее использовать в будущем при росте сети.
- ✓ **Безопасный доступ.** Выполнение автоматического резервирования означает, что устройство либо должно оставаться в сети, когда вы ушли, либо должно оставаться в системе при заблокированной клавиатуре. Выясните у поставщика, каким образом продукт регистрируется в сети и поддерживает ли функции безопасности.

Группа fiackufi Operators

Прежде чем пользователь сможет создать резервную копию или восстановить систему, он должен получить статус члена группы Backup Operators (Операторы архива). Это та же группа, что и группа Backup Operators в операционной системе Windows NT, но в системе Windows 2003 изменены процедура добавления пользователей к этой группе и политики группы. В зависимости от того, установлена ли в вашей системе Windows 2003 служба Active Directory или нет, шаги процедуры по добавлению пользователя к группе Backup Operators слегка отличаются.

По умолчанию в состав группы Backup Operators не входит ни одна учетная запись. Это просто пустой контейнер или "заместитель" на тот случай, если вам потребуется назначить пользователям права на резервирование и восстановление.

Чтобы изменить состав группы Backup Operators при отсутствии установленной службы Active Directory (другими словами, когда ваш сервер сконфигурирован как рядовой сервер, а не контроллер домена), выполните следующие действия.

1. **Выберите команду Start⇨Administrative Tools⇨Computer Management (Пуск⇨Администрирование⇨Управление компьютером).**
2. **В левой панели выберите узел Systems Tools (Служебные программы) и выделите пиктограмму Local Users and Groups (Локальные пользователи и группы).**
3. **В правой панели дважды щелкните на контейнере Groups (Группы).**

   Теперь в правой панели отображаются все группы, которые существуют в настоящий момент в вашей системе.

4. Выделите группу Backup Operators, дважды щелкните на ней и выберите опцию Add to Group (Добавить в группу).
5. Щелкните на кнопке Add (Добавить) и выберите пользователя или пользователей, которых вы намерены ввести в состав группы Backup Operators.
6. Щелкните на кнопке Add.
7. Щелкните на кнопке OK, затем щелкните на этой кнопке еще раз, чтобы закрыть диалоговое окно Backup Operators Properties.

Чтобы модифицировать состав группы Backup Operators при наличии установленной службы Active Directory, выполните следующие действия

1. Выберите команду Start⇨Administrative Tools⇨Active Directory Users and Computers.
2. В левой панели дважды щелкните на дереве, чтобы раскрыть его.
3. В правой панели дважды щелкните на папке Builtin (Встроенные).
4. В правой панели щелкните правой кнопкой мыши на группе Backup Operators и выберите пункт меню Properties.
5. Щелкните на вкладке Members.
6. Чтобы добавить пользователей, щелкните на кнопке Add.

Глава 18

Управление сетевой безопасностью

В этой главе...

- Основы сетевой безопасности
- Методы обеспечения безопасности в Windows Server 2003
- Применение пакетов обновления
- Выработка правильного отношения к безопасности
- Обнаружение и закрытие брешей в системе безопасности Windows 2003
- Обзор ресурсов безопасности

В развивающемся мире информационных технологий защита данных от назойливых глаз становится все более и более важной. Обеспечение безопасности, препятствующей доступу к внутренней информации, зачастую становится ключевым фактором конкурентного преимущества. В этой главе мы рассмотрим, как установить надежную защиту для Windows Server 2003.

Когда вы устанавливаете новую систему Windows Server 2003, она не обеспечивает полностью безопасную среду, поэтому вы должны сделать это. Этот процесс состоит из множества шагов, тщательного планирования, двойной проверки ваших установок и некоторых действий, не связанных напрямую с компьютерами. Если вы не заботитесь о безопасности данных, можете полностью пропустить эту тему.

Цель обеспечения безопасности заключается не в том, чтобы создать систему, которую не смогут взломать хакеры или повредить неумелые пользователи. Напротив, цель состоит в том, чтобы оградить ее достаточно высоким барьером от злоумышленников, чтобы трудности, с которыми они столкнутся при попытке доступа в вашу систему, были значительно выше, чем в какой-либо другой системе. Это напоминает возведение настолько высокой кирпичной стены вокруг вашего сада, чтобы у любого отбить охоту перелезать через нее (поэтому он полезет через забор вашего соседа). Ваша цель состоит в том, чтобы убедить хакера атаковать более легкую цель. Следуя рекомендациям, изложенным в этой главе, вы сможете развернуть систему Windows Server 2003, которую не только труднее взломать, чем соседнюю, но которая к тому же герметична!

Защита достояния и частной электронной собственности — это не только защита от атак извне, но также возведение барьеров, препятствующих нападениям изнутри, и принятие мер предосторожности против других угроз вашим данным.

Основы сетевой безопасности

Основное правило сетевой безопасности гласит: ненадежных людей следует держать подальше от сети, лишние данные должны быть удалены из сети, а необходимые данные — храниться строго внутри нее. Увольте нас от необходимости говорить об очевидности этого принципа.

Создание безопасной среды требует уделить внимание трем ключевым факторам.

- ✓ Знание операционной системы (или систем).
- ✓ Контроль физического доступа к компьютеру.
- ✓ Образование пользователей.

Эти три фактора подобны ножкам табуретки. Если одна из ножек подломится, человек свалится на пол.

В данном разделе мы кратко рассмотрим вопросы, связанные с поддержанием физического контроля и образованием пользователей. Третья ножка, собственно операционная система, станет предметом рассмотрения оставшейся части главы.

Физическая безопасность

Контроль физического доступа означает предотвращение присутствия людей, не имеющих на то разрешения, в непосредственной близости от вашего компьютера, сетевых устройств, линий коммуникаций, периферийных устройств и даже источников электропитания. Компьютерную систему можно подвергнуть риску несколькими способами. Физический доступ — это первый шаг к проникновению в систему. Помните, что физический доступ не всегда означает, что человек должен физически присутствовать в здании вашего офиса. Если ваша сеть оснащена коммутируемым доступом, кто-то может воспользоваться удаленным доступом.

Контроль физического доступа означает не только предотвращение доступа к клавиатуре или другим устройствам ввода, но также блокирование всех других средств передачи или получения сигналов от вашей компьютерной системы.

Некоторые способы контроля **физического** доступа очевидны для **всех.**

- ✓ Запирание дверей.
- ✓ Использованиеидентификационныхкарточек.
- ✓ Привлечение вооруженной охраны.
- ✓ Использование запирающихся кейсов и полок.

Если вы обратитесь только к этим элементам физической защиты, открытыми останутся некоторые другие методы доступа. Вам необходимо принять во внимание архитектуру, структуру и конструкцию вашего здания. Можно ли снять потолочные или этажные перекрытия, чтобы доступ можно было получить поверх стен или под ними? Позволяют ли вентиляционные шахты и окна проникнуть в запертые комнаты? Что, уже похоже на паранойю?

В поле вашего зрения должны попасть не только те люди, которые проникают в машинный зал. Вам также необходимо подумать о среде, в которой функционируют компьютеры. Для большинства компьютеров существует предельная температура, при которой они способны нормально работать. Поэтому если злоумышленники получат доступ к управлению термостатом, ваша система будет подвергнута риску. Что это за вещь, в которой нуждаются все компьютеры? Электричество. Защищена ли ваша система электропитания? Можно ли ее отключить за пределами ваших защитных барьеров? Оборудованы ли ваши важнейшие системы источниками бесперебойного питания?

Даже предохранив машинный зал от проникновения и защитив среду функционирования, вы по-прежнему не обеспечили своим компьютерам полную физическую защиту. Вам необходимо позаботиться о мусоре — да. о мусоре! Вы будете поражены тем, что могут узнать о вас и вашей сети частные следователи и преступники, пользуясь информацией, которая содержится в выброшенном вами мусоре. Если вы не разрежете или не сожжете все печатные и рукописные материалы, вы можете выдать пароли, имена пользователей, имена компьютеров, параметры конфигурации, пути к дискам и другую ключевую информацию.

Вы думаете, теперь мы охватили все? *Ошибаетесь!* Подумайте над следующими вопросами.

- ✓ Пылесосит ли и чистит ваше компьютерное помещение ночная бригада уборщиков?
- ✓ Можно ли поручиться за эту бригаду?
- ✓ Как часто бригада выключает компьютерные системы, чтобы включить уборочную машину?
- ✓ Открывается ли входная дверь тем же ключом, что и машинный зал?
- ✓ Вы уверены, что бригада уборщиков не играет на ваших компьютерах?
- ✓ Откуда вы знаете, что члены бригады уборщиков именно те, за кого себя выдают?
- ✓ Установлены ли на серверах и других важнейших системах дисководы для гибких магнитных дисков?
- ✓ Можно ли перезагрузить системы без использования пароля или других средств идентификации (например, смарт-карты)?
- ✓ Имеются ли на серверах дополнительные порты, готовые для подключения к ним новых соединений?
- ✓ Сложены ли ваши ленты с резервным копиями на лентопротяжном устройстве?
- ✓ Защищены ли ваши ленты с резервными копиями шифром и паролями?
- ✓ Учитываются ли все ваши ленты с резервными копиями? Если некоторые не учтены, знаете ли вы, какая информация на них хранится?
- ✓ Что в действительности происходит в здании вашего офиса после работы? Запираются ли двери каждую ночь?

Если вы все еще способны спать по ночам, значит, большая часть этих вопросов находится под вашим контролем. Если вы не можете твердо и уверенно ответить на некоторые из этих вопросов, вам следует кое-что предпринять.

Вопросы физического доступа, которые мы обсуждали до сих пор, касались стационарных компьютерных систем. А как быть с мобильными рабочими станциями? Вы помните о дорогостоящей системе ноутбук, которую вы купили для вашего шефа, менеджера и системного администратора, так что теперь они могут работать в пути и подключаться к сети по телефонной линии? Хорошо, если один из этих ноутбуков не попадет в руки того, кто сможет открыть "двери", чтобы прямо попасть в вашу сеть и взять или разрушить все, что им заблагорассудится.

Хищение ноутбуков становится способом номер один для получения доступа к сетям компаний. Большинство ноутбуков похищается в аэропортах. (Готовы поспорить, что вы так и подумали!) Хотя большая часть путешественников достаточно сообразительна, чтобы не регистрировать свои ноутбуки в качестве багажа, есть одно место, где ноутбук и его хозяин часто разделяются — металлодетектор. Проходит всего несколько минут в ожидании прохождения сквозь рамку металлодетектора после того, как вы поместили ноутбук на транспортер рентгеновского аппарата, но за то время, пока вы дошли до другого его конца, ноутбук исчез.

Контроль физического доступа важен, поскольку без взаимодействия с компьютерной системой хакер не сможет ее взломать. Если вы пренебрегаете предотвращением физического доступа в вашу сеть, то единственное, на что вам остается полагаться при защите ваших данных, — это на поддерживаемое операционной системой ПО обеспечения безопасности. Однако здесь существует одна проблема — если ваши сетевые пользователи недостаточно образованы, сетевая безопасность может пострадать.

Информирование масс

Самая защищенная сетевая среда бесполезна, если пользователи не осознают необходимости защиты. В действительности, будучи предоставлены самим себе, большинство людей при выполнении повседневной работы идут по пути наименьшего сопротивления. Другими словами, ваши пользователи делают все для того, чтобы упростить прохождение системы защиты, например автоматизируют ввод пароля, записывают пароли на видном месте, устанавливают отображения для несанкционированных дисков, устанавливают не получившее одобрения ПО, переносят данные с работы домой и назад на дискетах и подключают модемы в обход брандмауэров и proxy-серверов. Если вы внедрите меры безопасности на основе соответствующего ПО или средств ОС, люди зачастую могут отыскать пути обойти их или по меньшей мере снизить их эффективность.

Образование пользователей — двойственный процесс. Во-первых, пользователи вашей сети должны досконально знать, что такое безопасность, почему она так важна и какие меры безопасности применяются в вашей сети. Во-вторых, нарушения системы безопасности со стороны пользователей должны немедленно и сурово пресекаться.

В большинстве случаев обучение сетевых пользователей требует выпуска специального официально-распорядительного документа, который уточняет ограничения и требования системы безопасности, равно как и наказания за ее нарушение. Этот документ носит название *политики безопасности (security policy)* и служит основным законом сети. Он определяет все основные нормы и положения сетевой безопасности. Этот документ позволяет сохранить в целости систему безопасности и при этом пресечь деятельность нарушителей закона.

Итак, что необходимо знать пользователям о системе сетевой безопасности вашей организации? Ниже приводится краткий перечень основных положений.

- ✓ Используйте пароль правильно и выбирайте его разумно. (Не используйте очевидных имен или цифр, например клички ваших домашних любимцев или дату своего рождения).
- ✓ Никогда не записывайте пароль и не делитесь им с другими.
- ✓ Никогда не делитесь идентификационными карточками или жетонами и не оставляйте их без присмотра.
- ✓ Предоставляйте доступ к сети только уполномоченным работникам.
- ✓ Не делитесь информацией об учетных записях с другими работниками или с кем-либо вне организации.
- ✓ Не распространяйте данные из сети в любой форме вне организации.
- ✓ Пользователи не должны отходить от компьютеров, если только они подключены к системе.
- ✓ Умейте объяснить наличие различных уровней сетевой безопасности и назначение такого разделения.
- ✓ Не устанавливайте ПО, не одобренное руководством организации.
- ✓ Доведите до сведения всех работников, что противодействие, подрыв или пренебрежение мерами безопасности является основанием для увольнения.
- ✓ Соблюдайте тайну организации и других пользователей.
- ✓ Нарушение политики безопасности должно незамедлительно и жестко пресекаться без оговорок и исключений.

Здесь мы подходим к вопросу наказания. Если пользователь нарушил существенное положение политики безопасности, к нему необходимо применить строгое наказание. В большинстве случаев увольнение работника является единственной формой наказания, которая позволяет эффективно контролировать ситуацию и удерживает других пользователей от совершения аналогичной ошибки. Повторение нарушения политики безопасности должно найти отражение в самой политике. И если уж вы вынесли наказание, будьте последовательны до конца. Даже если нарушителем является ваш главный программист, он должен нести столь же суровое наказание, что и временный почтовый работник.

Большинство аналитиков пришли к выводу, что внедрение жесткой политики безопасности приводит к обычному явлению — кратковременному улучшению безопасности, за которым следует короткий период расслабления, приводящий в итоге к нарушениям, в результате чего несколько человек увольняют, что немедленно приводит к общему продолжительному улучшению в области безопасности. В своих отчетах компании указывают, что потери в людских ресурсах из-за нарушений незначительны в сравнении предупреждением появления брешей в системе безопасности.

Вы должны выработать свою собственную политику безопасности, которая включает детали, касающиеся физического контроля, образования пользователей и мер безопасности на уровне операционной системы. Помните, что легче предупредить болезнь, чем лечить ее.

Windows 2003 и безопасность

Безопасность Windows Server 2003 концентрируется вокруг контроля доступа. Контроль доступа зависит от идентичности пользователя, которая определяется пользовательской учетной записью пользователя, Чтобы получить доступ к компьютеру или сети, работающей под управлением Windows Server 2003, вы должны предоставить пользователю учетную запись пользователя, которая содержит допустимое имя пользователя и пароль. Любой, кто знает допустимую комбинацию имени пользователя и пароля, может получить доступ. Поэтому необходимо защищать как имя пользователя, так и пароль.

Имена пользователей - это не просто имена

Безопасно защитить имена пользователей не всегда просто, однако с помощью небольших усилий удается отразить некоторые виды легких атак. Во-первых, не создавайте имена пользователей, в которых используется имя или фамилия человека. Во-вторых, при создании имени используйте комбинацию двух или более элементов наподобие имени, фамилии, инициалов, кода отдела или названия подразделения. Не используйте также для входа в систему имя, которое используется в качестве адреса электронной почты пользователя. Это несколько затрудняет процесс угадывания имен пользователей. Даже если хакер знает ваше соглашение об именовании, создание замысловатых имен пользователей может затруднить грубую силовую атаку. (Соглашение об именовании более подробно рассматривалось в главе 15.)

Вы также должны переименовать общие учетные записи: Administrator (Администратор), Guest (Гость) и IUSR_<имя сервера> (создаваемая информационной службой Internet — IIS). После переименования имена этих учетных записей должны носить описательный характер, но при этом они не должны легко вычисляться.

Затем создайте новую мнимую учетную запись с оригинальным именем, в которой будут отсутствовать какие-либо права доступа. Она должна служить приманкой для хакеров, заставляя их тратить время впустую, а вам даст больше возможностей выяснить, кто они на самом деле.

Ваша политика безопасности должна содержать ограничения, препятствующие применению пользователями их сетевых регистрационных имен в качестве регистрационных имен где-либо

еще. Другими словами, пользовательское сетевое регистрационное имя не должно использоваться как регистрационное имя для входа на Web- и FTP-узлы (File Transfer Protocol — протокол передачи файлов) или в другие внешние системы. Если пользователи не используют то же регистрационное имя где-либо еще, у них будет меньше соблазн использовать где-либо еще и пароль.

Даже с учетом этих предосторожностей имена пользователей зачастую поддаются раскрытию. Здесь важным вопросом является как можно более затруднить получение любых элементов данных, необходимых для входа в вашу сеть. После раскрытия имени пользователя защита сети зависит только от неприступности вашего пароля.

Пароли и безопасность

С помощью пароля можно предотвратить несанкционированный доступ к системе. Чем надежнее пароль, тем больше вероятность того, что система безопасности останется неповрежденной. В качестве составляющей политики безопасности вы должны требовать от каждого пользователя использовать хорошо защищенный пароль. (О том, как создать защищенный пароль, рассказывается в конце этого раздела.) Взлом одной учетной записи может привести к открытию доступа ко всей системе.

Надежно защитить пароль можно с помощью встроенных элементов управления Windows 2003. Применение элементов управления системного уровня, которые обеспечивают надежные пароли, потребует лишь небольших дополнительных усилий, чтобы добиться от пользователей соблюдения политики безопасности.

Политики учетных записей определяют ограничения, требования и параметры политик паролей, блокирования учетных записей и системы Kerberos. Чтобы получить доступ к политикам учетных записей, выполните следующие действия.

1. **Выберите команду Start⇨Administrative Tools⇨Active Directory Users and Computers (Пуск⇨Администрирование⇨Пользователи и компьютеры Active Directory).**
2. **Выберите имя вашего домена.**
3. **Выберите команду Action⇨Properties (Действие⇨ Свойства).**

   Появится диалоговое окно свойств домена.
4. **Щелкните на вкладке Group Policy (Политика групп).**
5. **Выберите опцию Default Domain Policy (Политика умолчания** домена), **а затем щелкните на кнопке Edit (Модифицировать).**

   Появится диалоговое окно Group Policy Object Editor (Редактор объекта политики группы).
6. **Под узлом Computer Configuration (Конфигурация компьютера) раскройте элемент Windows Settings (Параметры Windows).**
7. Под узлом **Windows Settings раскройте элемент Security Settings (Параметры безопасности).**
8. **Под узлом Security Settings раскройте элемент Account Policies (Политики учетных записей).**

Теперь в левой панели окна Local Security Settings (Параметры локальной безопасности) вы увидите политики паролей (Password Policy), блокирования учетных записей (Account Lockout Policy) и системы Kerberos (Kerberos Policy).

Политика пароля

Отыскав опцию Account Policies (Политики учетных записей), вы можете получить доступ к политике пароля с помощью команды Account Policies⇨Password Policy (Политики учетных записей⇨Политика пароля). Шесть опций, показанных на рис. 18.1, позволяют вам контролировать требования к паролям пользователей. Чем выше вы поднимаетесь по "ступеням" из шести опций, тем более строгими становятся требования к паролю, так что вероятность успеха лобовой атаки против вашей системы становится все меньше и меньше.

В приведенном ниже перечне мы кратко поясняем каждую из возможностей, разъясняем принимаемые по умолчанию установки и рекомендуем наиболее приемлемые установки для использования в общем случае.

- ✓ **Enforce password history (Требовать неповторяемости паролей).** Значение по умолчанию равно 3. Мы рекомендуем устанавливать значение 5 и больше, которое означает, что система хранит 5 паролей, применяемых пользователями, так что никто из них не сможет повторно воспользоваться каким-либо из этих паролей.
- ✓ **Maximum password age (Максимальный срок действия пароля).** Значение по умолчанию равно 42 дням. Эта опция используется для определения момента истечения срока действия и смены пароля, Мы рекомендуем использовать значения 30, 45 и 60 дней.
- ✓ **Minimum password age (Минимальный срок действия пароля).** Значение по умолчанию равно 0. Эта опция используется для определения продолжительности ожидания пользователем смены своего пароля. Мы рекомендуем применять значения 1, 3 и 5 дней.
- ✓ **Minimum password length (Минимальная длина пароля).** Значение по умолчанию равно 0. Эта опция используется для определения наименьшего количества символов, из которых должен состоять пароль. Мы рекомендуем использовать для пароля как минимум 6 символов.

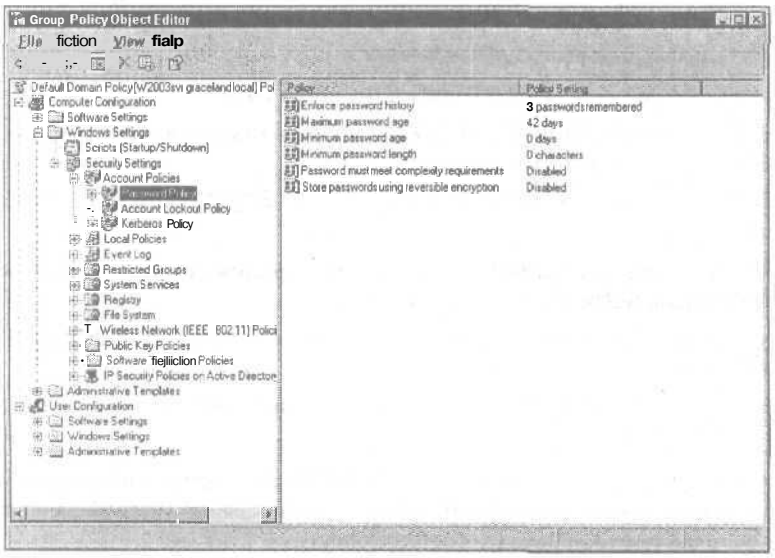


Рис. 18.1. Изменение политики пароля с использованием средства управления политикой групп

- ✓ **Passwords must meet complexity requirements (Пароли должны отвечать требованиям сложности).** Значение по умолчанию — Disabled (Отключен). Требования сложности находят отражение в правилах, требующих, к примеру, использовать в пароле как прописные, так и строчные буквы, числа и алфавитно-цифровые символы. Если выработанные вами требования к паролю недостаточны, мы рекомендуем провести дальнейшее изучение требований к сложности с использованием возможностей справочной системы Windows 2003 и пакета Resource Kit для Windows Server 2003.
- ✓ **Store password using reversible encryption for all users in the domain (Хранить пароли всех пользователей в домене, используя обратимое шифрование).** Значение по умолчанию — Disabled (Отключен). Включение этого атрибута позволяет использовать протокол аутентификации пароля Shiva (Shiva Password Authentication Protocol — SPAP), представляющий собой механизм идентификации безопасности для протокола PPP (Point-To-Point Protocol — протокол двухточечного соединения), разработанного корпорацией Shiva. Этот атрибут следует оставить отключенным, если только клиент не требует использования протокола SPAP.

Политика блокирования учетных записей

Следующей среди политик учетных записей является политика блокирования учетных записей (Account Lockout Policy), которая управляет блокированием учетной записи пользователя в результате повторных неудачных попыток регистрации (выберите команду Account Policies⇨Account Lockout Policies (Политики учетных записей⇨Политика блокирования учетных записей). Блокирование препятствует лобовым атакам (при которых вводят все возможные или вероятные пароли) за счет отключения учетной записи пользователя. Ниже перечислены соответствующие опции.

- ✓ **Account lockout threshold (Пороговое значение блокировки).** Значение по умолчанию равно нулю неверных попыток регистрации. Эта опция используется для определения числа неверных попыток регистрации, приводящего к блокировке. Мы рекомендуем значения от 3 до 5 неверных попыток регистрации.
- ✓ **Account lockout duration (Блокировка учетной записи на).** Значение по умолчанию — Not Defined (Не определено). Эта опция используется для определения продолжительности блокировки учетной записи. Присваивание атрибуту значения Forever (Всегда) требует вмешательства администратора для разблокирования учетной записи, Мы рекомендуем устанавливать для этого параметра значение 30 минут и больше.
- ✓ **Reset account lockout counter after (Сброс счетчика блокировки через).** Значение по умолчанию — Not Defined (Не определено). Эта опция используется для определения интервала времени, по истечении которого счетчик неверных попыток регистрации для одной учетной записи переустанавливается. Мы рекомендуем значение для этого атрибута, равное 15 минутам.

Политика Kerberos

Последняя среди политик учетных записей — политика Kerberos, которая управляет работой защищенного сеанса связи (выберите команду Account Policies⇨ Kerberos Policies (Политики учетных записей⇨Политика Kerberos). Kerberos — усовершенствованный протокол сетевой идентификации. С помощью протокола Kerberos клиенты могут единожды идентифицировать себя в начале сеанса связи, а затем выполнять множество задач во время этого сеанса, не идентифицируя себя повторно. Другими словами, Kerberos используется для подтверждения идентичности клиента серверу и наоборот. После проведения проверки идентичности сеансы связи можно начинать без повторения этого процесса (либо, как минимум, до момента разрыва связи).

Вот опции для этой политики.

- ✓ **Enforce User Logon Restriction** {) — Enabled (Включен).
- ✓ **Maximum lifetime for user ticket renewal** () — 7 дней.
- ✓ **Maximum lifetime for service ticket** () — 600 минут.
- ✓ **Maximum tolerance for computer clock synchronization** 0 — 5 минут.
- ✓ **Maximum lifetime for user ticket** () — 10 часов.

Более подробно о системе Kerberos для Windows 2003 вы можете узнать, обратившись на Web-узел Microsoft, посвященный Windows 2003 и безопасности (www.microsoft.com/net/technical/security.asp), и на Web-узел Microsoft, посвященный безопасности (www.microsoft.com/security).

Кое-что о паролях из нашего опыта

Позволяете ли вы программным элементам управления ограничивать пароли или нет, мы рекомендуем включать в организационную политику безопасности следующие элементы.

- ✓ Применяйте минимум шесть символов.
- ✓ Препятствуйте тому, чтобы адреса электронной почты, имена учетных записей или реальные имена были частью пароля.
- ✓ Не используйте обычных слов, сленга или терминов.
- ✓ Не записывайте пароли, за исключением случаев, когда они хранятся в сейфах или безопасных банковских ячейках.
- ✓ Не используйте слова, имена или фразы, которые могут ассоциироваться с вами, связанные с вашей семьей, друзьями, увлечениями, домашними любимцами, интересами, книгами, фильмами, автомобилями или рабочей средой.
- ✓ При использовании реальных слов разделяйте их прописными буквами, цифрами или символами, отличными от алфавитно-цифровых, например Go7Ril-la.
- ✓ Используйте цифры или отличные от алфавитно-цифровых символы для замены букв, например 13EE33r
- ✓ Используйте по меньшей мере три из четырех типов символов: прописные, строчные буквы, цифры, специальные символы (например, знаки пунктуации).
- ✓ Создавайте аббревиатуры из предложений в качестве паролей, например "Fifty-five dollars will pay a parking ticket" - 55DwPaPt.

Посредством сочетания навязываемых Windows 2003 ограничений и правил политики безопасности компании вы можете повысить безопасность вашей системы за счет использования хорошо защищенных паролей.

Взгляд в будущее: пакеты обновления

Компания Microsoft регулярно выпускает обновленные и исправленные версии своих продуктов, называемые *выпусками "заплаток" (patch release)*. Так она поступала с Windows NT и Windows 2000, то же, вероятно, будет и с Windows 2003. Поскольку "заплатки", выпускаемые Microsoft, призваны исправлять все виды ошибок, устранять проблемы и решать другие вопросы, мы предполагаем, что некоторые из "заплаток" обращены к проблемам, связанным с безопасностью. Поэтому важно быть в курсе выпуска и содержания этих "заплаток".

Компания Microsoft выпускает "заплатки" в двух формах: пакеты обновления и "горячие исправления". *"Горячее исправление "* (*hotfix*)— это "заплатка" для одной проблемы. *Пакет обновления* (или *служебный пакет — service pack*) — это несколько "горячих исправлений", сведенных в единый пакет поддержки. Существует также много и более существенных различий. "Горячие исправления" полностью не тестируются и не поддерживаются Microsoft. "Горячее исправление" должно применяться только в том случае, если вы действительно столкнулись с проблемой, которое оно исправляет, поскольку "горячее исправление" иногда само вызывает проблемы. Пакеты обновления тщательно тестируются и поэтому более безопасны для развертывания. Однако мы рекомендуем воздерживаться от применения пакета обновления примерно на два месяца с момента его появления. Это дает оставшейся части сообщества пользователей Windows 2003 время на установку и тестирование "заплатки" для вас. Всегда лучше учиться на ошибках других, чем набивать шишки самому.

Пакеты обновления — кумулятивные, а это значит, что каждый новый выпуск пакета обновления включает предыдущие пакеты обновления и все "горячие исправления" и другие усовершенствования, внесенные со времени их выпуска. Используйте только самый последний пакет обновления и все требуемые "горячие исправления".

Прежде чем применить какую-либо "заплатку" к Windows 2003, вы должны прочитать документацию, которая прилагается к ней. Затем выполните следующее.

- ✓ Создайте резервную копию системы или, по меньшей мере, ваших данных и реестра.
- ✓ Перезагрузите систему.
- ✓ Закройте все приложения и приостановите выполнение всех лишних служб.

Если вы не знаете в точности, какой уровень пакета обновления используете, вы можете проверить это, взглянув на информационную страницу (Help⇨About (Справка⇨О программе)) из любого "родного" для Windows 2003 приложения (наподобие Windows Explorer (Проводник), Control Panel (Панель управления) или My Computer (Мой компьютер)).

В прошлом Web-узел Microsoft держал в тайне местоположение пакетов обновления и "горячих исправлений", однако недавно компания стала намного более открытой. Лучше всего отыскать пакет обновления посредством программы Windows Update (которая находится в разделе All Programs меню Start и присутствует в виде команды в меню Tool программы Internet Explorer). Вы также можете посетить раздел загрузки Web-области Windows 2003, расположенный по адресу `www.Microsoft.Com/WindowsServer2003/`.

Быть хозяином положения

Для сопровождения защищенной сетевой среды вы должны быть пессимистом. Смотрите на каждого пользователя как на потенциальную брешь в защите и предоставляйте только тот требуемый уровень доступа, который необходим пользователям или группам для выполнения их рабочих заданий. Чтобы довести эту философию до логического завершения, вам необходимо работать с группой Everyone и правами пользователей.

Группа Everyone

Группа Everyone (Все) создается по умолчанию системой и включает всех определенных и анонимных пользователей. Хотя это и не "сборная солянка", каковой она была в Windows NT 4.0, всеобъемлющий характер группы по-прежнему может привести к проблемам безопасности, поскольку Windows 2003 по умолчанию предоставляет права на чтение новых томов и сетевых ресурсов группе Everyone. Это значит, что вам необходимо неусыпно следить за появлением этих групп в вашей системе. Вы можете предоставить неограниченные права там, где вы и близко в действительности не желаете ничего подобного.

Кажется, что за трупной Everyone трудно уследить. Она не появляется в списке встроенных групп и ее можно увидеть, например, посредством утилиты Active Directory Users and Computers. Однако она присутствует в списке групп при настройке параметров безопасности объектов. Группу Everyone нельзя удалить из системы, однако ею можно эффективно управлять, не прилагая больших усилий, Более подробно о группе Everyone рассказывалось в главе 15.

Группа Authenticated Users представляет собой стандартное средство Windows 2003. Она содержит всех определенных пользователей, но не содержит анонимных пользователей. Возможно, вам потребуется использовать группу Authenticated Users вместо группы Everyone, если понадобится предоставить неограниченный доступ. Группа Everyone должна присутствовать в вашей системе для обеспечения обратной совместимости и требований системного уровня (наподобие позволения вашей системе загружаться).

Не устанавливайте все разрешения для группы Everyone равным Deny, поскольку этим вы помешаете получить всем пользователям доступ к ресурсам. Вместо этого удалите группу Everyone из списка пользователей и групп, которым разрешен доступ.

При создании нового диска или общедоступного ресурса удалите группу Everyone, а затем добавьте только тех пользователей и группы, которым необходим доступ к ресурсу. Поскольку вы не намерены предоставлять доступ к вашему компьютеру кому угодно, вы не должны разрешать доступ всем к областям, где это не требуется.

Права пользователей

Права пользователей — это полномочия системного уровня, контролирующие тип выполняемых им действий. Устанавливаемые по умолчанию права пользователей обеспечивают достаточный уровень безопасности, но вы можете несколько его улучшить. Доступ к интерфейсу управления правами пользователей можно получить с использованием редактора политики групп (см. выше раздел "Пароли и безопасность"). Опции назначения прав пользователей расположены под узлами Security Settings⇨Local Policies⇨User Rights Assignments (Параметры безопасности⇨Локальные политики⇨Назначение прав пользователя). Посредством этого интерфейса можно назначить права пользователей и отменить их. Ниже приводится перечень некоторых изменений в правах, которые вам стоит принять во внимание.

1 ✓ **Удалите группу Guests из контейнера прав Allow Log on Locally (Разрешить локальный вход в систему).** Это изменение препятствует получению несанкционированного доступа.

✓ **Удалите группу Everyone из** контейнера **прав Access This Computer from the** Network **(Доступ к данному компьютеру из сети).** Это изменение препятствует получению неуполномоченными пользователями доступа к ресурсам компьютера через сеть.

✓ **Удалите группу Everyone из контейнера прав Bypass Traverse Checking (Контроль обходного пути).** Это изменение препятствует переходу неуполномоченных пользователей к подкаталогам, к родительским каталогам которых они не имеют доступа.

if ✓ **Удалите группу Backup Operator (Оператор архивирования) из контейнера прав Restore Files and Directories (Восстановление прав и каталогов).** Это изменение препятствует неадминистраторам восстанавливать файлы с резервных лент. Поскольку файлы можно восстановить в разделы файловой системы FAT при утере списков контроля доступа ACL (Access Control List), это — важное изменение, повышающее уровень безопасности системы,

После внесения этих изменений дважды проверьте, чтобы рядовые пользователи по-прежнему имели возможность выполнять свои повседневные задачи. Вам может потребоваться предоставить эти пользовательские права лишь немногим пользователям и группам. Например, если вам необходимо предоставить пользователям доступ к ресурсам сервера через сеть, вы должны добавить группу, такую как Users, в контейнер прав Access This Computer from the Network.

Латание прорех

Windows 2003 присущи некоторые бреши в системе безопасности, которые вы не должны упускать из виду и закрывать. К счастью, мы досконально изучили эти проблемы, так что вам не придется повторять наш путь. Просто следуйте нашим дружеским советам, и вы будете чувствовать себя в безопасности.

Невидимые административные общедоступные ресурсы

При каждой загрузке Windows 2003 для каждого диска создается скрытый общедоступный ресурс. Эти общедоступные ресурсы представляют собой резервные пути для системы на тот случай, если непосредственный доступ к системным файлам будет некоторым образом ограничен. Другими словами, это ненужная вам избыточность! Административные общедоступные ресурсы отключаются с помощью добавления параметра AutoShareServer в следующий ключ реестра:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServser
\Parameters"
```

Значение параметра, равное 0, отключает административные общедоступные ресурсы, а значение, равное 1, вновь возвращает их. Подробности, касающиеся отключения административных разделяемых ресурсов, можно узнать, обратившись к сетевому ресурсу Microsoft TechNet.

Скрытый разделяемый ресурс подобен любому другому разделяемому ресурсу, за исключением того, что в качестве последнего символа его имени используется знак доллара. Это информирует систему о том, что не следует отображать скрытый разделяемый ресурс в стандартном списке просмотра общедоступных ресурсов. Для просмотра скрытых разделяемых ресурсов вы можете использовать утилиту System Manager. Вы можете создать свои собственные скрытые разделяемые ресурсы, добавив знак доллара в конец имени разделяемого ресурса.

Проблема с административными общедоступными ресурсами состоит в том, что они предоставляют неограниченный доступ к каждому файлу на диске. Если имя пользователя и пароль администратора каким-либо образом оказались раскрыты, этот ресурс может быть использован кем угодно для отображения любого административного общедоступного ресурса в сети. Поэтому целесообразно отключить административные общедоступные ресурсы в качестве предупредительной меры.

Учетные записи-приманки

Всем известны имена наиболее важных учетных записей вашей системы. Поскольку Windows Server 2003 при установке создаст учетную запись Administrator, все уже знают ее точное имя и то, что вы обладаете такой учетной записью. Поэтому вам следует изменить ее!

Не изменяйте только имя. Лучше создайте новую фиктивную учетную запись, которая не обладает никакими правами доступа или полномочиями вообще, и дайте ей имя администратора. Фиктивная учетная запись служит приманкой, призванной отвлечь внимание хакеров от получения реального доступа.

Создание ловушек для других общих учетных записей, таких как учетная запись Guest и IUSR (которая создается службой IIS), — также неплохая идея.

Последний зарегистрировавшийся пользователь

По умолчанию после нажатия комбинации клавиш <Ctrl+Alt+Del>диалоговое окно входа в систему отображает имя пользователя, который зарегистрировался последним. Это не самая безопасная установка. Чтобы предотвратить появление диалогового окна, включите опцию Interactive logon: Do not display last user name policy (Не отображать политику последнего имени пользователя). Эта опция располагается в области Secure Options объекта Group Policy (о том, как отыскать эту область, см. выше, в разделе "Права пользователей"),

Когда хороший флоппи-диск вреден

Отличное средство, которое можно загрузить **с Web-узла Systems Internals** (www.sysinternals.com), **позволяет кому угодно прочитать** NTFS-файлы **после загрузки** системы **с флоппи-диска DOS. Драйверы** NTFSDOS делают **возможным то, что по заявлению Microsoft невозможно. Теперь любой человек, обладающий физическим** доступом **к вашей** системе, **может перезагрузить систему с флоппи-диска и скопировать файлы с** ваших **защищенных** дисков NTFS. **Если вы дорожите своими данными (и вашей работой),** удалите **флоппи-дисководы из наиболее важных систем.**

Безопасность равносильна бдительности

Сопровождение безопасной среды — непрерывный процесс. Как правило, поддержка исправлений ошибок в системе безопасности, системных изменений, деятельности пользователей и политик — трудоемкая задача. В плане ваших работ по поддержке защищенного развертывания Windows 2003 выделите время, чтобы ознакомиться с содержимым следующих Web-узлов, групп новостей **и** других **ресурсов.**

- **Web-страница проблем безопасности и секретности Microsoft** (www.microsoft.com/security/).
- **Партнеры Microsoft в области безопасности** (http:/members.microsoft.com/partner/partnering/programs/SecuritySolutions/).
- **Журнал Windows &.Net Magazine** (www.winntmag.com).
- **Somarsoft** (www.somarsoft.com/).
- **@stake** (www.atstake.com/).
- **Координационный центр CERT** (www.ct.org/).
- **BHS Software** (www.bhs.com/).
- **Корпорация Xtras** (www.xtras.net/).
- Microsoft TechNet (www.microsoft.com/technet/).

Ниже приведен список книг издательской группы "Диалектика-Вильяме", которые также могут оказаться полезными. (Да, большинство названий содержат *Windows 2000.* В большинстве случаев информация по-прежнему применима к Windows 2003. Однако вы не должны упускать из виду новых изданий, которые посвящены Windows 2003.)

- *Microsoft Windows 2000 Security Handbook* (Справочник по безопасности *Microsoft Windows 2000),* Джефф Шмидт (Jaff Schmidt), издательство Que.
- *Configuring Windows 2000 Server Security* (Настройка конфигурации безопасности Windows 2000) (издательство Snygress Media).
- *Windows Server 2003 Security Little Black Book* (Маленькая черная книжечка по безопасности Windows Server 2000), Эдвард Остин (Edward Austin) (издательство Coriolis Group).
- *Maximum Security* (Максимум безопасности) (издательство Sams.net).
- *Firewalls and Internet Security: Repelling the Wily Hacker* (Брандмауэры и безопасность Internet: отражение хитрого хакера), Уиьям Р. Чесвик (William R. Cheswick) и Стивен М. Белловин (Steven M. Bellovin) (издательство Addison-Wisley).
- *Building Internet Firewalls* (Построение брандмауэров Internet), Брент Д. Чепмен (Brent D. Chapment) и Элизабет Д. Цвики (Elithabeth D. Zwicky) (издательство O'Reilly&Associates).
- *Система безопасности Windows 2000.*
- *Архитектура брандмауэров для сетей предприятия.*
- *Обнаружение нарушений безопасности в сетях, 3-е издание.*
- *Секреты хакеров. Безопасность сетей — готовые решения, 4-е издание.*
- *Руководство по защите от хакеров.*
- *Защита от хакеров. Анализ 20 сценариев взлома.*

Часть V

Выявление и устранение проблем

"Наша автоматизированная политика реагирования на широкомасштабную потерю данных большими компаниями состоит в уведомлении руководства, резервировании существующих данных и продаже 90% моих акций компании".

В этой части...

Несмотря на ваши лучшие намерения и все предупреждения на свете, сети подвержены случайностям. Иногда они даже вообще перестают работать, и именно тогда требуются средства отыскания проблем. В части V вы узнаете, что обнаружение неполадок — это скорее направление мыслей, чем какой-либо конкретный набор испробованных и проверенных средств, приемов и методов решения проблем.

Часть V открывается обзором основных утилит Windows 2003 для обнаружения проблем и продолжается рассмотрением аналогичных средств, которые помогут вам справиться с сетевыми проблемами. После этого вы познакомитесь с тем, как разрешить проблемы, возникающие из-за бездеятельности или "странностей" Active Directory.

Часть V охватывает важные основы обнаружения неисправностей машины, работающей под управлением Windows Server 2003, и сети, к которой она подключена. Мы не описываем все проблемы, а рассматриваем лишь хорошо известные (или, по крайней мере, наиболее часто встречающиеся).

Обнаружение неполадок — это то, с чем приходится время от времени сталкиваться всем. Помните, что следует не паниковать, а систематически анализировать к симптомы. Вы должны стремиться выявить характер заявившей о себе проблемы прежде, чем сможете понять, что подойдет в конкретном случае. Фиксируйте проблемы и их решения по мере того, как вы встречаетесь с ними и корректируете их. Таким образом вы сможете не только решить большинство проблем самостоятельно, но и создать базу знаний, которая поможет вам в дальнейшем.

Глава 19

Использование утилит Windows 2003 для устранения проблем

В этой главе...

- Использование утилиты Event Viewer
- Разбор аварийных дампов
- Возможности System Information Tool
- Работа с утилитой Computer Management для Windows 2003
- Отображение производительности с помощью Performance Monitor
- Анализ утилит Resource Kit

Хотя утверждение "где Windows Server 2003 — там и проблема" не всегда оправданно, тем не менее система Windows Server 2003 вполне может быть источником проблем. По мере чтения этой главы вы ознакомитесь с самыми распространенными и неизвестными средствами выявления неполадок в системе, которые предлагает Windows 2003.

В конце этой главы мы кратко остановимся на некоторых утилитах пакета Resource Kit для обнаружения неисправностей, достойных внимания.

Что позволяет обнаружить Event Viewer

Утилита Event Viewer (Просмотр событий) — важный инструмент выявления проблем для Windows Server 2003. Вы всегда можете рассчитывать на то, что Event Viewer предоставит вам массу подробностей о том, что происходит, когда драйверы или службы отказываются загружаться при запуске системы. Утилита Event Viewer — это также исходный пункт вашего анализа происходящего с системой, независимо от того, анализируете ли вы конкретные события или пытаетесь выявить источник возникших проблем или ошибок.

Для запуска утилиты Event Viewer выберите пункты меню Start⇨Administrative Tools⇨Event Viewer (Пуск⇨Администрирование⇨Просмотр событий). В результате откроется диалоговое окно Event Viewer, показанное на рис. 19.1.

В правом столбце различных журналов Event Viewer отображаются следующие пиктограммы.

- ✓ **Красный кружок со значком X.** Известна как пиктограмма ошибки и указывает на отчет об ошибке, которую, может быть, стоит проанализировать.
- ✓ **Голубой пузырек со строчной буквой *i*.** Называется информационной пиктограммой и указывает на событие, которое описывает успешную операцию службы основного сервера.
- ✓ **Желтый треугольник с восклицательным знаком.** Известна как пиктограмма предупреждения и указывает на появление события, которое не обязательно является серьезным, но может свидетельствовать о наличии потенциальных проблем. Эта информация также может заслуживать более пристального рассмотрения.

Чтобы проанализировать некоторый элемент журнала, дважды щелкните на строке, в которой он появился. После того как мы дважды щелкнули на одном из красных кружков, показанных на рис. 19.1, появился отчет утилиты Event Viewer о подробностях события (рис. 19.2).

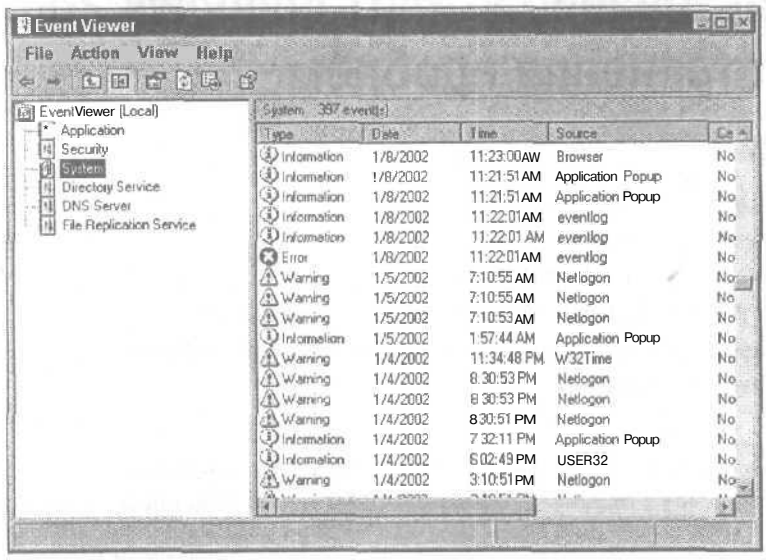


Рис. 19.1. Вид системного журнала в утилите Event Viewer

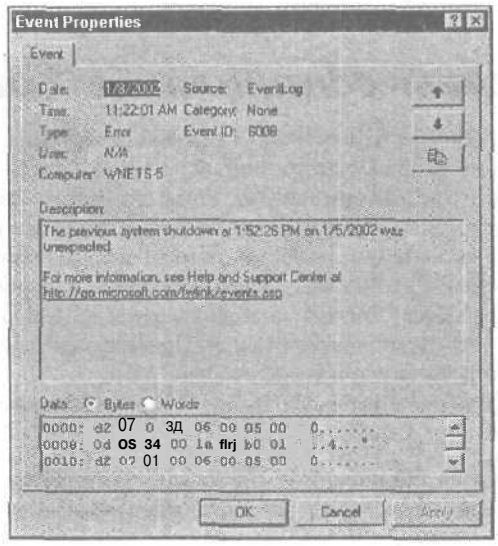


Рис. 19.2. Подробности событий

Журнал системы (System) появляется в диалоговом окне утилиты Event Viewer по умолчанию. Утилита также включает три других основных файла журналов (помимо журнала системы) и может включать журналы для конкретных служб и приложений, в зависимости от того, какие приложения и службы установлены в вашей системе. Ниже приведен сокращенный список журналов, которые отображаются утилитой Event Viewer для нашей тестовой системы.

- **Application Log (Журнал приложений).** Фиксирует события, регистрируемые некоторыми приложениями или службами. При создании приложения разработчики могут заложить в него как часть инсталляции возможность отправки информации о событии утилите Event Viewer. Пиктограмма, которая появляется в журнале приложений, аналогична пиктограмме системного журнала.
- **Directory Services (Служба каталогов).** Фиксирует события, связанные со службой каталогов.
- **DNS Server (Сервер DNS).** Фиксирует события, связанные с сервером службы имен доменов.
- File **Replication Service** (Служба **архивирования файлов).** Фиксирует события, связанные со службой архивирования файлов.
- **Security Log (Журнал безопасности).** Фиксирует события, связанные с безопасностью, наподобие изменений в политике безопасности машины и неудачных попыток входа в систему или доступа к файлам и каталогам. Именно в этом журнале регистрируется информация аудита системы безопасности. Журнал безопасности использует две специальные пиктограммы: желтый ключ указывает на успешное завершение события аудита безопасности, серый замочек указывает на то, что аудит события, связанного с безопасностью, завершился неудачей.
- **System Log (Журнал системы).** Фиксирует все события, регистрируемые системными компонентами Windows 2003. По умолчанию системный журнал регистрирует все ошибки, предупреждения и информационные сообщения, связанные с оборудованием и операционной системой.

Работа с утилитой Event Viewer должна стать частью вашей повседневной деятельности по сопровождению системы. Проверяйте журналы приложений и системы по меньшей мере раз в неделю, чтобы выяснить, не произошло ли что-нибудь неблагоприятное для системы, Аудит событий системы безопасности связан с проверкой журнала безопасности, и его следует проводить так часто, как это диктует необходимость.

"Толстое" приложение? Зовите доктора Ватсона!

В этой книге вы встретитесь со множеством средств и утилит выявления проблем, связанных с оборудованием, сетями и самой операционной системой Windows 2003. Но что делать, если ваше приложение ведет себя скверно?

Ответ на этот вопрос звучит так: "Ничего!" Не потому, что вы ничего не можете сделать с проблемами, вызванными приложениями, а потому, что подобные проблемы в среде Windows 2003 автоматически вызывают отчеты об ошибках, генерируемые утилитой Dr. Watson. В действительности функция утилиты Dr. Watson состоит в том, чтобы сообщать о возникновении трудностей, с которыми сталкиваются приложения.

Хотя вы, вероятно, не желаете знать, что делать с содержимым отчетов утилиты Dr. Watson, — если только вы не обладаете достаточным опытом программирования в среде Windows и не знакомы с отладчиками, — будьте уверены, что для большинства людей это совершенно бесполезная вещь. От вас же занятие с утилитой Dr. Watson потребует проверки места размещения аварийного дампа, создания копии этого дампа и отправки его по почте тому, кто (может быть) сумеет сделать из всего этого что-нибудь путное! Что касается аварийного дампа, то его описание содержится в текстовом поле "Crash Dump" окна приложения Dr. Watson, которое отображается с помощью ввода в поле ввода текста команды Run строки drwtsn32.

Если приложение ведет себя скверно, утилита Dr. Watson может оказаться весьма полезной для персонала технической поддержки, которая может попробовать найти средство от "болезни" вашей системы.

В процессе обнаружения проблем утилита Event Viewer должна быть первым средством. Помимо снабжения информацией о большинстве проблем системы, на этот инструмент можно положиться как на источник информации, касающейся проблем любого приложения или службы, которое знает, как использовать эту возможность для генерации предупреждений и сообщений об ошибках. К сожалению, это не относится ко всем приложениям, но включает большую часть служб серверов и наиболее важных приложений, таких как системы управления базами данных и пакеты электронной почты.

Разбор дампа

Если вам придется когда-нибудь иметь несчастье самому выявлять ошибку в Windows 2003, то, надо сказать, что это трудный процесс, который начинается с таинственных отказов сервера и затем превращается в долгие, тягостные обращения к персоналу технической поддержки компании Microsoft. Поэтому вам, вероятно, потребуется создать аварийный дамп, чтобы персонал мог воспользоваться им.

Чтение аварийного дампа выходит далеко за пределы круга обязанностей обычного системного или сетевого администратора. Вам просто необходимо различать этот термин и знать, как создать аварийный дамп для некоего эксперта, который рассмотрит его в свободное время.

Начнем с определения. *Аварийный дамп (crash dump)* — это мгновенный снимок всей оперативной памяти, который выполняется в случае, когда система Windows 2003, настроенная на регистрацию аварийного дампа, действительно терпит аварию. Он включает информацию об операционной системе, оборудовании, о приложениях, а также другие типы информации, которую Windows 2003 держит в скрытом виде и использует для управления своим собственным функционированием.

Эксперт может разобрать аварийный дамп, чтобы точно указать причины аварии и использовать свои знания для формирования исправлений или обходных путей. Это один из источников создания "заплаток" и исправлений, которые постепенно появляются в пакетах обновления, — на тот случай, если вы удивляетесь, откуда берутся подобные вещи.

Для включения функции аварийного дампа ваш компьютер должен удовлетворять следующим критериям.

- ✓ Файл подкачки должен размещаться в том же разделе, где размещаются системные файлы Windows 2003. На языке Windows 2003 это называется *загрузочным разделом (boot partition)*. Файл подкачки вносит свой вклад в общий аварийный дамп и должен быть доступен после завершения работы системы — это значит, что он должен находиться на том же диске, что и утилита аварийного дампа.
- ✓ Вы должны располагать достаточным объемом свободного пространства на загрузочном диске, чтобы зафиксировать все содержимое оперативной памяти, а также файла подкачки. Это значит, что суммарный объем свободного пространства должен быть равен сумме указанных объемов (ОП и файла подкачки). Чтобы определить необходимый объем свободного пространства, откройте диалоговое окно Task Manager (Диспетчер задач), щелкните на вкладке Performance (Быстродействие) и обратите внимание на значение, представленное в поле Limit (Предел) панели Commit Charge (Выделение памяти). Чтобы запустить диспетчер задач, щелкните правой кнопкой мыши на любой области панели задач и выберите в контекстном меню пункт Task Manager. В этом поле представлен объем свободной памяти в килобайтах, который вам необходим (чтобы получить значение в мегабайтах, разделите это число на 1024).

После того как эти критерии будут удовлетворены, включите функцию аварийного дампа в диалоговом окне Startup and Recovery (Запуск и восстановление). Для отображения этого диалогового окна выберите команду Control Panel⇨System (Панель управления⇨Система), щелкните на вкладке Advanced (Дополнительно), а затем щелкните на кнопке Settings (Параметры) в области Startup and Recovery. Раздел Write Debugging Information (Записывать отладочную информацию) содержит выпадающий список, в котором вы можете выбрать возможность записи файла небольшого дампа, дампа только ядра системы, файла полного дампа или вообще ничего не записывать. Имя файла дампа по умолчанию (`%systemroot%\MEMORY.DMP`) определяется в диалоговом окне Dump File (Файл дампа). Вам нет необходимости изменять это значение. Диалоговое окно Startup and Recovery показано на рис. 19.3.

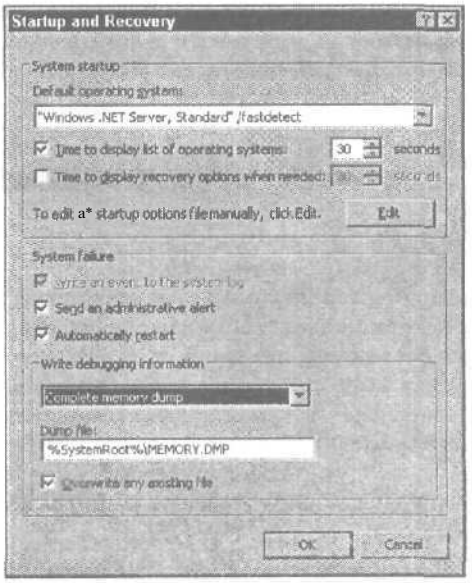


Рис. 19.3. Установка параметров для аварийного дампа

Теперь, когда параметры файла дампа выбраны, при наступлении в системе события ошибки STOP (серьезная ошибка, которая, если ее не устранить, может привести к порче данных) она записывает файл MEMORY.DMP в системный каталог Windows 2003. По умолчанию значение символа `%systemroot%\` равно `C:\WINDOWS` в предположении, что вы установили Windows Server 2003 на диск `C:` с принятым по умолчанию именем корневого системного каталога.

Аварийный дамп порождает две интересные проблемы. Во-первых, поскольку суммарный объем ОП и файла подкачки, вероятно, составляет 200 Мбайт и больше, вы должны найти способ передать копию файла в службу технической поддержки. (Лучше всего в этом случае наличие быстродействующего канала Internet.) Во-вторых, вы должны удалить этот файл после создания копии; в противном случае ваш сервер, вероятно, выйдет за пределы пространства загрузочного раздела.

Сжатие аварийного дампа обычно позволяет уменьшить его объем на 70% или более, так что мы рекомендуем вам перед отправкой упаковать его (используя такую утилиту, как WinZip, которую можно найти на Web-узле `www.winzip.com`).

Сведения о системе

Может быть, вы помните инструмент Windows NT Diagnostics из Windows NT 4.0, который теперь называется System Information (Сведения о системе). В системе Windows 2000 это средство входило в состав утилиты Computer Management (Управление компьютером), а в Windows 2003 оно помещено в подраздел System Tools меню Start (Start⇨All Programs⇨Accessories⇨System Tools⇨System Information (Пуск⇨Программы⇨Служебные⇨Служебные программы⇨Сведения о системе)). Раскрыв пять подразделов раздела System Summary (Сведения о системе), Hardware Resources (Ресурсы аппаратуры), Components (Компоненты), Software Environment (Программная среда), Applications (Приложения) и Internet Settings (Параметры Internet), вы можете получить подробную информацию о состоянии, параметрах, конфигурации и функционировании системы. Именно сюда стоит заглянуть перед тем, как добавлять новое оборудование, или при попытке найти причину отказа устройства.

Оснастка Computer Management Windows 2003

С внедрением технологии Plug and Play и консоли управления Microsoft (Microsoft Management Console — MMC) некоторые функции и приложения, входившие в состав Windows NT 4.0 и Windows 9.x, были объединены для создания многоцелевого инструмента контроля для Windows 2003. Инструмент Computer Management (Управление компьютером), диалоговое окно которого показано на рис. 19.4, предоставляет вам доступ к средствам выявления проблем наподобие System Information (Сведения о системе) и Device Manager (Диспетчер устройств). Чтобы получить доступ к интерфейсу средства управления компьютером, выберите команду Start⇨Administrative Tools⇨Computer Management (Пуск⇨Администрирование⇨Управление компьютером).

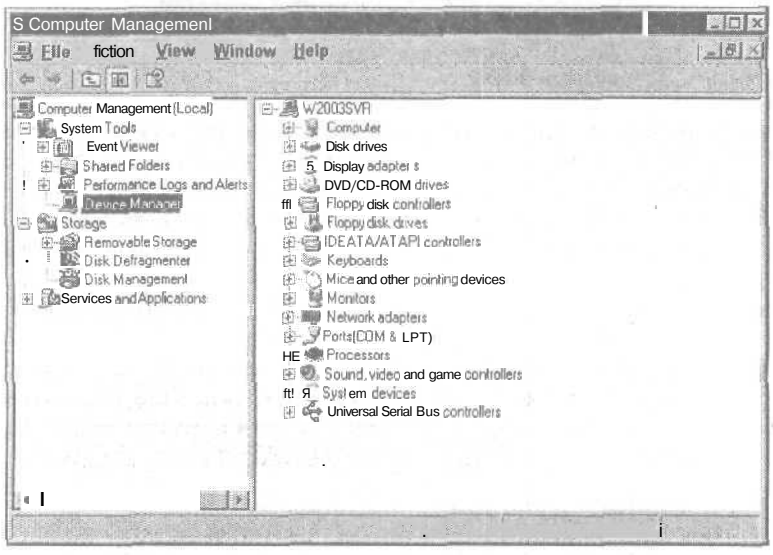


Рис. 19.4. Инструмент Computer Management

Компонент управления устройствами Device Manager заимствован из системы Windows *9.x* (и является средством, о котором просили пользователи Windows NT). Это отличное средство содержит полный список установленных устройств. После раскрытия заголовков с типами устройств в правой панели для получения перечня отдельных устройств вы можете дважды щелкнуть на имени любого из устройств, чтобы открыть диалоговое окно Properties (Свойства). С помощью этого диалогового окна вы можете выполнить следующее.

- ✓ Получить информацию о состоянии устройства.
- ✓ Запустить справочную программу для обнаружения неполадок.
- ✓ Удалить или заменить драйверы,
- ✓ Изменить параметры конфигурации.
- ✓ Изменить специфические для устройства параметры функционирования.

В дальнейшем вы имеете возможность изменять конфигурацию устройства на лету. И во многих случаях, чтобы изменения вступили в силу, вам нет необходимости перезагружать систему.

Монитор производительности

Утилита мониторинга быстродействия Windows 2003 (которая теперь называется System Monitor (Системный монитор) представляет собой недооцененное творение вдохновенного гения. Мы утверждаем это не только потому, что это справедливо, но и потому, что мы прониклись доверием к этому отличному инструменту, который помогал нам в устранении всех типов проблем на протяжении нескольких лет.

Когда утилита System Monitor запускается впервые (Start⇨Administrative Tools⇨ System Monitor (Пуск⇨Администрирование⇨Системный монитор), она по умолчанию представляет показания трех счетчиков (рис. 19.5). За счет небольших усилий по планированию утилита System Monitor может предоставить много полезной информации, касающейся производительности компьютерной системы и сети.

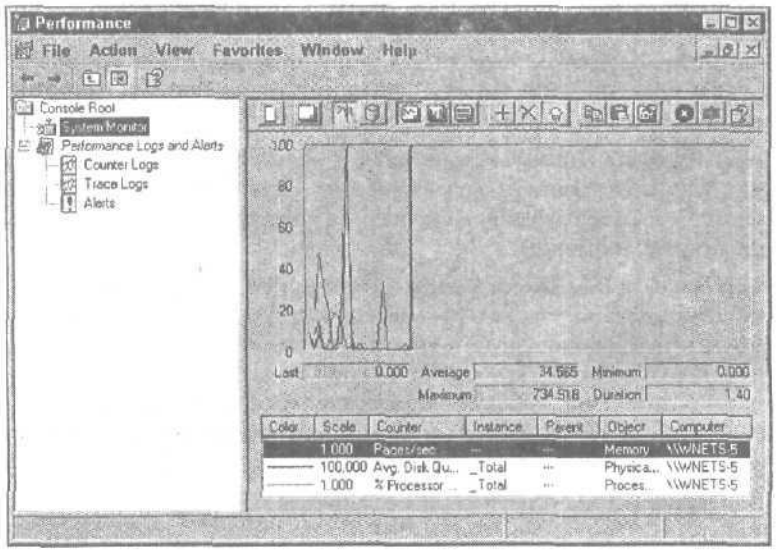


Рис. 19.5. Утилита Performance Monitor

Вы используете основное отображение утилиты System Monitor для наблюдения за измерениями производительности, которые выполняются в реальном времени либо предварительно зафиксированы. В зависимости от того, на какой кнопке панели инструментов вы щелкнете, область отображения может представить измерения в графической форме (наподобие ЭКГ), в виде гистограммы (например, термометра) или в виде отчета (например, бюджета). Дополнительную информацию о системном мониторе можно получить в главе 20.

Подсчет объектов

Производительность измеряется на основе счетчиков и объектов. Некоторые подробности, касающиеся объектов Windows 2003, были рассмотрены в главе 16. В данной главе все, что вам необходимо знать, сводится к тому, что в среде Windows 2003 все рассматривается как объект и каждый объект обладает своими собственными счетчиками, которые измеряют определенные аспекты производительности или действий этого объекта. Полные сведения о производительности включают следующее.

- ✓ Компьютер. Система-источник объекта.
- ✓ Объект. Подсистема, представляющая определенный интерес.
- ✓ Счетчик. Аспект производительности, представляющий интерес.
- ✓ Экземпляр. Специальный объект, который подлежит измерению, если в одной системе существует несколько объектов одного типа.

Счетчики можно добавить к области отображения, щелкнув на кнопке с изображением большого знака "плюс" на панели инструментов System Monitor. На экране отобразится диалоговое окно Add Counters (Добавить счетчики), в котором вы можете выбрать контекст счетчиков, которые вы намерены отобразить. Если в этом диалоговом окне щелкнуть на кнопке Explain (Пояснить), отобразятся детали, касающиеся выбранного счетчика.

Ниже приводится перечень наиболее важных для отслеживания пар объект-счетчик (в приводимом списке имя объекта показано слева, за ним следует обратная косая черта, затем — имя счетчика).

- ✓ **Server\Bytes Total/sec (Сервер\Байт** всего/с). Показывает, какой объем данных обрабатывает сервер за определенное время (для базового измерения степени загрузки вашей системы). Другие счетчики для объекта сервера, такие как Sessions Errored Out, Work Item Shortage, Errors System и Blocking Request Rejected, могут указывать на потенциальные узкие места в системе.
- ✓ **Memory\Pages/sec (Память\Страниц/с).** Показывает, насколько часто сервер перемещает данные из памяти на диск и наоборот. Если эта величина принимает большие значения (более 2500 страниц в секунду для среднего сервера), это может указывать на нехватку ОП на сервере.
- ✓ **PhysicalDisc\Avg.Disc** Queue **Lenght** (Физический **диск\Длина** средней очереди к диску). Указывает на то, сколько запросов к диску ожидает обслуживания. Если эта величина в течение длительного времени остается на уровне 2.0, это может свидетельствовать о том, что дисковое устройство слишком медленное, чтобы справиться с подобной нагрузкой, либо это устройство "задавлено" текущими дисковыми операциями. Иногда это говорит о необходимости установки более быстрого устройства, или дискового контроллера, или даже более быстрой дисковой подсистемы.

Объекты, используемые для наблюдения за работой дисков, могут вызвать проблемы с производительностью, даже если утилита System Monitor не записывает информацию о них. Поэтому по умолчанию Windows 2003 включает только счетчики для физических дисков PhysicalDisc и блокирует счетчики для логических дисков (LogicalDisc). С помощью инструмента командной строки DISKPERF вы можете заблокировать или разблокировать оба дисковых объекта. Более полную информацию, касающуюся использования этих объектов, можно получить с помощью ввода команды `diskperf /?` в строку приглашения для ввода команд.

Легкое чтение на лето

Существует много книг по вопросам мониторинга и настройки производительности Windows NT 4,0 и Windows 2000, и мы уверены, что вскоре появится немало аналогичных книг по Windows 2003. Большинство советов, применимых к Windows NT 4,0 и Windows 2000, также применимо и к Windows 2003, однако они могут быть полезны в разной степени.

Ниже перечислено несколько книг, которые мы обычно рекомендовали для мониторинга производительности Windows NT 4.0 и Windows 2000.

- ✓ Windows 2000 Performance Guide (Руководство по производительности Windows 2000), Марк Фридман (Mark Friedman) (издательство O'Reilly & Associates).
- ✓ Windows 2000; Performance Tuning & Optimization (Windows 2000: настройка и оптимизация производительности), Кентон Гардинер (Kenton Gardinier) (издательство Osborne/Mcgraw-Hill).
- ✓ Windows NT Server 4.0 Secrets (Секреты Windows NT Server 4.0), Валд Хиллей (Vald Hilley) (издательство Wiley Publishing, Inc.).

Обратите внимание на этих авторов; возможно, они опубликуют книги с аналогичными названиями для Windows 2003.

Обратитесь на Web-узел `www.amazon.com`, использовав в качестве поисковой строки **Windows 2000 Performance**, и вы можете натолкнуться на некоторые книги, которые еще не вышли на момент написания этой книги. Удачи вам!

Журналы и предупреждения

Основную пользу от утилиты System Monitor можно получить посредством ее регистрационных журналов. С помощью журналов вы имеете возможность зафиксировать данные о производительности, которые сможете проанализировать позже. Это не только позволит собирать данные в широких временных рамках без необходимости сидеть и наблюдать за процессом, но и является хронологической основой для создания базиса, выявления проблем и планирования мощности системы.

Чтобы создать файлы журналов, выберите узлы Counter Logs (Журналы счетчиков) и Trace Logs (Журналы трассировки) в главном окне утилиты Performance. Журналы Counter Logs используются для записи измерений определенных счетчиков (а не просто объектов в целом). Журналы Trace Logs используются для записи событий, связанных с памятью и ресурсами.

Чтобы создать файлы журналов, выберите узлы Counter Logs и Trace Logs в левой панели, щелкните правой кнопкой мыши в правой панели и выберите пункт меню New Log Settings (Новые параметры журнала). Вам необходимо присвоить имя файлу журнала и определить элементы, которые он будет фиксировать. Например, вы можете назвать файл сервера 1-2-2-02-cpu.log и записывать измерения объекта центрального процессора. После записи файла журнала вы можете просмотреть его содержимое в окне утилиты System Monitor, щелкнув на кнопке View Log Data (Просмотр данных журнала) панели инструментов.

Еще одно полезное свойство утилиты System Monitor (может быть, не столь значительное) проистекает из возможности определять предупреждения. Предупреждения позволяют администраторам отдать команду утилите System Monitor следить за определенными счетчиками и

отправлять сообщение в случае достижения некоторого заранее заданного значения. Администраторы используют вид Alerts (Предупреждения) для выдачи предупреждений в случае медленной работы диска или при опасно высокой загрузке сети или центрального процессора. Вид Alerts можно рассматривать в качестве своего рода возможности выдачи системных предупреждений. Событие Alerts генерируется в случае превышения значения счетчика некоторого порогового значения и выполняет следующие функции.

- ✓ Запись элемента в журнал приложений инструмента Event Viewer.
- ✓ Отправка сетевого сообщения.
- ✓ Выполнение пакетного файла.
- ✓ Запуск регистрации данных о производительности.

Вы можете определить предупреждения в области Alerts главного окна утилиты System Monitor. Выберите компонент Alert в левой панели, щелкните правой кнопкой мыши в правой панели и выберите пункт меню New Alert Settings (Новые параметры предупреждения).

Утилиты Windows 2003 Resource Kit

Многие программисты и инженеры, которые помогали разрабатывать Windows 2003, создали инструменты и утилиты, которые никогда не входили в официальный выпуск продукта Windows 2003. Многие из этих инструментов, позволяющих сэкономить время и избавить пользователей от головной боли, включены в пакет Windows Server 2003 Resource Kit наряду со множеством технических деталей и приемов, которые отсутствуют *в* руководствах и интерактивных справочниках.

Пакет Windows Server 2003 Resource Kit был включен в дистрибутивный компакт-диск предварительного выпуска с основной операционной системой, но мы не знаем, поставляется ли он на компакт-диске, содержащем окончательный вид операционной системы. Если он отсутствует на компакт-диске, у вас есть возможность найти его в книжном Internet-магазине или на Web-узле TechNet (`www.microsoft.com/technet/`).

Вы обнаружите в пакете Resource Kit сотни утилит выявления проблем. Мы приводим краткий список категорий соответствующих ресурсов и советуем детально изучить их.

- ✓ Computer Management Tools (Инструменты управления компьютером). Включает широкий набор утилит проверки, контроля и профилирования.
- ✓ **Deployment Tools (Инструменты развертывания).** Включает утилиты для развертывания операционной системы Windows Server 2003 и ПО общего назначения, в том числе специальные средства, такие как инструмент мониторинга SID (Security Identifier — идентификатор безопасности) и средства подготовки системы.
- ✓ **Diagnostic** Tools (**Инструменты диагностики).** Включает утилиты для мониторинга или инспекции приложений, сетевой операционной системы и сети.
- ✓ **Network Management Tools (Инструменты управления сетью).** Включает утилиты для службы каталогов, возможностей взаимодействия сетей, администрирования сетей, управления производительностью, удаленными вычислениями и памятью.
- ✓ **Registry Tools (Инструменты управления реестром).** Включает в избытке средства работы с реестром, которые можно использовать для выполнения операций командной строки, например для создания уникальных очередей для значений; добавления, изменения или удаления значений; копирования подразделов и операций резервирования и восстановления.

- ✓ **Win32 Debugger Tools (Средства отладки Win32).** Включает утилиты для программистов для выявления проблем и отладки программ, разрабатываемых под заказ, а также отладки ПО, разработанного для платформы Windows 2003.

Чтобы узнать больше об этих утилитах, обратитесь к файлу RKTOOLS.CHM на компакт-диске с утилитами Resource Kit или отыщите установленную папку (\Program Files\Resource Kit). Этот файл содержит пояснения для каждой из утилит!

Глава 20

Избавляемся от сетевых проблем

В этой главе...

- Что случается, когда сеть "ведет" себя плохо
- Анализ симптомов
- Утилита NetMon
- Двойной контроль сетевых установок
- Поиск потерявшегося сервера
- Медленная сеть
- Доступ к сети
- Устранение перемежающихся проблем

Даже при самом лучшем планировании, отлично подобранном оборудовании и присутствии самого лучшего администратора сети время от времени терпят аварию. Отследить неприятность лучше до того, как она случится, но знать, как быстро исправить положение после того, как она произошла, может быть спасением. Современные неоднородные сетевые среды зачастую ставят перед пользователями и администраторами трудные задачи. В этой главе мы рассмотрим некоторые распространенные сетевые проблемы и расскажем, как их решать.

Когда tfosttuicatotfi сетевые проблемы

Чтобы уменьшить вероятность возникновения сетевых проблем, вы должны усвоить предупреждающие знаки, связанные с сетевыми проблемами, и предпринимать планово-предупредительные меры.

Поскольку сеть состоит из большого количества ресурсов, то когда работа сети разлаживается, то же самое происходит с Internet-соединениями, электронной почтой, факсами и устройствами печати. Э, да тут, кажется, дело идет к полной "аварийной остановке" бизнеса! Так и есть на самом деле, нарушение работы сети может вызвать множество проблем для организации.

Что значит исправная сеть? Создание базиса

Один из способов отслеживать сеть на предмет возникновения проблем заключается в том, чтобы создать базисный отчет о том, как выглядит сеть в те дни, когда она работает надлежащим образом. Если вы считаете, что сеть функционирует плохо, можете сравнить "моментальные снимки" сети в удачный и неудачный день. Некоторые администраторы предпочитают делать базисную "моментальную фотографию", а затем еженедельный "моментальный снимок". Вы можете отслеживать сетевую память, процессор, вход пользователей в сеть и ее использование, поскольку эти области, как правило, содержат предупреждающие признаки, которые показывают, что с сетью что-то неладно. Вы можете отслеживать эти функции с помощью инструмента System Monitor, который поставляется вместе с системой Windows Server 2003. Выберите команду Start⇨Administrative Tools⇨Performance

(Пуск⇨ Администрирование ⇨Быстро действие). Открывшееся диалоговое окно Performance содержит две функции: System Monitor (Системный монитор) и Performance Logs and Alerts (Оповещения и журналы производительности).

В диалоговом окне System Monitor (Системный монитор) вы можете просматривать информацию в реальном времени или информацию по загрузке, которую вы зарегистрировали раньше.

В диалоговом окне Performance Logs and Alerts можно просматривать различные журналы в текстовом формате, чтобы анализировать каждое отдельное предупреждение. В действительности это не устаревший простой ASCII-формат; это по-прежнему графический интерфейс пользователя (GUI), но предупреждения выводятся как линейные элементы, которые вы можете просматривать и фильтровать.

Чтобы добавить счетчики и объекты, щелкните правой кнопкой мыши на кнопке Counters (Счетчики) в нижней части диалогового окна и выберите опцию Add Counters (Добавить счетчики). Вы можете также щелкнуть на кнопке Add (Добавить) с изображением знака "плюс" в правой панели. Появится диалоговое окно Add Counters (рис. 20.1). Ваш компьютер по умолчанию выбирается для мониторинга, но вы можете осуществлять мониторинг какого-либо другого компьютера вашего домена. Затем вам необходимо выбрать объект, производительность которого вы будете измерять, например объект Processor (Процессор), который выбирается по умолчанию, Print Queue (Очередь печати) или Paging File (Файл подкачки). При выборе объекта для оценки производительности отображаются счетчики для этого объекта. После выбора счетчика вам может потребоваться выбрать экземпляр, если в вашей системе находится больше одного объекта данного типа. Например, если на вашем компьютере установлено больше одного жесткого диска, вы выбираете тот, за которым намерены наблюдать.

Вы можете проверить сервер, процессор и память на предмет общего количества входов в систему, количества входов в систему в секунду, объема используемой памяти и того, насколько используется наличная пропускная способность сервера. Если вам не понятно назначение конкретного объекта или счетчика, щелкните на кнопке Explain (Объяснение), чтобы получить дополнительную информацию.

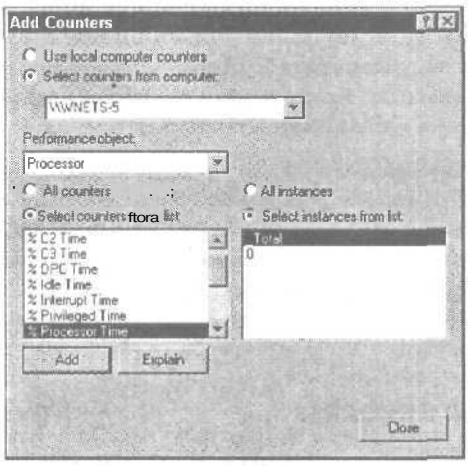


Рис. 20.1. Диалоговое окно ***Add Counters***

Пока диалоговое окно Add Counters отображается на экране, вы можете добавить столько счетчиков производительности, сколько требуется. По мере добавления счетчиков они принимают цвет, который затем приобретают график и легенда внизу диаграммы. Щелкайте на кнопке Add и выбирайте объекты до тех пор, пока не закончите, после этого щелкните на

кнопке Close (Закрыть). На рис. 20.2 показано окно System Monitor после того, как мы добавили несколько счетчиков и приступили к мониторингу. Обратите внимание на график изменения производительности в реальном времени (с интервалом в одну секунду).

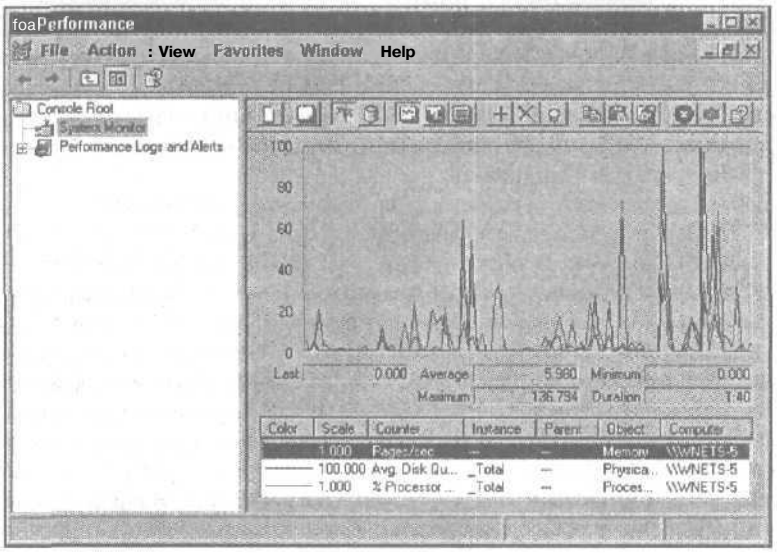


Рис. 20.2. График, построенный системным монитором

Когда вы приступаете к использованию Windows Server 2003, необходимо установить базис. Затем настройте предупреждения и счетчики для слежения за производительностью в течение интервалов пиковой нагрузки или в других временных рамках. Это позволит вам проводить анализ загрузки сети и сервера после некоторого периода эксплуатации. Внесите изменения в настройки сервера, а затем вновь обратитесь к журналам, чтобы понять, помогли ли изменения. Например, если вы установили, что на сервере требуется больше памяти, добавьте память, а затем вновь просмотрите журналы, чтобы убедиться в том, что это изменение повысило производительность. Кроме памяти вам может потребоваться поэкспериментировать с некоторыми другими настройками.

Поскольку вы намерены отслеживать поведение сервера на регулярной основе, сохраните настройки конфигурации (File⇨Save as (Файл⇨Сохранить как)) и введите имя файла, например `Perfset.msc`. Затем при наблюдении за сервером вы можете воспользоваться вашими сохраненными настройками конфигурации. Если вы сохраните настройки на рабочем столе, Windows 2003 создает пиктограмму, на которой вы можете щелкнуть в следующий раз для наблюдения за сервером с этими параметрами.

Документирование проблем

Мы рекомендуем вам запастись блокнотом и записывать все, что связано с сетевыми проблемами (желательно делать это вместе с появлением проблемы или сразу после ее возникновения). Вы должны фиксировать симптомы, элементы, которые вы изменили для устранения проблемы, а также дату и время. Документирование может послужить вам опорой, если в результате внесенных вами изменений выйдет из строя что-нибудь другое. Например, вам может потребоваться дать пользователю А разрешение на работу с приложением по обработ-

ке электронных таблиц. Затем, неделю спустя, вы заметили, что файл основного шаблона изменен этим пользователем и все пользователи вашей сети жалуются, что их приложения по обработке электронных таблиц имеют новые настройки по умолчанию. Возможно, вы дали этому пользователю слишком большие права.

В эту документацию вам следует включить рисунок вашей сети (называемый *сетевой схемой*). Общий взгляд на сеть поможет вам обнаружить и устранить неполадки, поскольку вы можете обозревать разные сегменты и относящуюся к ним информацию. Подробную информацию о сетевых схемах см. в главе 5.

Если у вас есть машинный зал, вы должны запирать дверь и требовать от посетителей заполнять журнал посетителей — даже человек, который пришел сменить электрическую лампочку на потолке, должен заполнять его, поскольку лестница может задеть некоторые провода в машинном зале и нарушить работу сегмента сети.

В некоторых организациях, в которых работают несколько сетевых администраторов, мы наблюдали, что пока один администратор устраняет одну проблему, другой впускает специалиста по обслуживанию в машинный зал. Когда с сетью происходит что-то неладное, сетевые администраторы начинают искать проблему, но не знают, что кто-то побывал в машинном зале. Если вы ограничиваете доступ ко всему вашему оборудованию насколько возможно, точно знаете, кто ходит рядом с этим оборудованием, и регистрируете все изменения, у вас будет больше шансов быстро устранить неполадки.

Если в вашей организации больше одного сетевого администратора и возникла какая-то неисправность, соберите всех, чтобы задать следующие вопросы.

- ✓ Вносил ли кто-нибудь сегодня какие-либо изменения, которые не были зарегистрированы?
- ✓ Был ли кто-либо из посторонних в машинном зале?

Затем проверьте журнал изменений в сети, чтобы понять, могут ли изменения в сети, произведенные в течение последней недели, каким-либо образом связаны с возникшей проблемой.

Взгляд с высоты в 30 тысяч футов

Когда ваша сеть отказывает, попробуйте отступить назад и взглянуть на нее с расстояния. Не поддавайтесь начинающейся панике, поскольку это не поможет вам понять что к чему, Разделите сеть на сегменты так, чтобы вы могли проанализировать, какая из частей сети вышла из строя: одна рабочая станция, один сегмент, один сервер, одно приложение или одна служба? После того как вы изолируете проблему, можете исправлять ее.

Если эта сеть связана с глобальной сетью, объем вашей работы возрастает. Кто-то мог внести изменения в глобальную сеть, которые сказались на вашей сети. Если вы подключены к глобальной сети, убедитесь в использовании схем уникального именования и адресации. Если все дают своим серверам Windows 2003 и доменам одинаковые имена (например, Server1, Server2, Server3 и т.д.), трудно надеяться на нормальную работу сети. Например, вы можете установить Windows Server 2003 изолированно (не подключая ее к какой-либо сети), а впоследствии подключить ее к глобальной сети. Если не применять никакой схемы именования, другие серверы глобальной сети могут обладать такими же именами и адресами, что действительно может привести к срыву работы сети.

Помимо использования схем уникального именования и адресации вам необходимо создать в глобальной сети резервные пути или связи на случай отказа связей. Если этого не сделать, вы можете обнаружить, что удаленные офисы вам недоступны до тех пор, пока сеть не будет восстановлена. Связи могут отказать из-за проблем среды или вышедшего из строя оборудования на вашей стороне.

В некоторых случаях вам может потребоваться разорвать соединение с глобальной сетью, чтобы убедиться в том, что от ближайшей проблемы вы избавились.

Если вы используете службу Active Directory и не управляете каталогом надлежащим образом, может оказаться, что локальная сеть связана с другими сетями через глобальную сеть, которая мешает работе вашей сети. Поэтому разорвите глобальное соединение, чтобы убедиться в исчезновении неисправности.

Блок-схемы помогут диагностировать проблемы, поскольку стимулируют ваше логическое мышление (конечно, если блок-схемы — логические). Изобразите блок-схему вашего метода обнаружения неисправностей и держите ее под рукой, чтобы при возникновении проблемы взглянуть на нее и быстро определить ее источник.

Раскройтеистину и удивитесь!

Вы должны не только следить за общим состоянием вашего сервера и сети, но также обходить весь офис и говорить с пользователями. Мы обнаружили, что пользователи не докладывают о неполадках так часто, как нам хотелось бы. Иногда вы сталкиваетесь с пользователями, которые случайно рассказывают вам о проблеме, которая заставляет их несколько раз на день перезагружаться. Пользователи просто мирятся с этим и не докладывают вам. Мы склонны рассматривать "прогулки по этажу" как часть нашей обшей схемы сетевого мониторинга.

Сеть становится медленнее... совсем медленной

Замедление работы сети сразу вызывает подозрение о существовании некоторой проблемы, причину которой следует начинать выискивать в дисковом пространстве и памяти сервера Windows Server 2003. Неисправный сетевой адаптер рабочей станции также может привесит к замедлению, поскольку сеть пытается обойти отказавшую плату. Для отслеживания и сбора информации о неполадках вы можете использовать утилиты System Monitor и Network Monitor (NetMon). Если в вашей сети установлен интеллектуальный концентратор, который собирает статистику в соответствии с протоколом SNMP (Simple Network Management Protocol — упрощенный протокол сетевого управления) на централизованную консоль управления, также обратитесь к этому журналу. Зачастую они графически показывают сетевой адаптер рабочей станции, который барахлит.

Утилита NetMon

NetMon — утилита Windows Server 2003, которая позволяет отыскивать данные в сети способом, напоминающим работу анализатора протокола. Вы можете настроить компьютер, работающий под управлением Windows Server 2003, на получение из сети кадров с последующим анализом того, что происходит на уровне ошибки, на уровне протокола и т.д. К сожалению, утилита NetMon не настолько развита, чтобы вы смогли просматривать всю сеть. Вы можете просматривать только входящие кадры для компьютера, работающего под управлением Windows Server 2003, на котором вы установили программный агент и инструментальные средства. Если вы желаете просматривать кадры в рамках всего сетевого сегмента, то должны использовать NetMon для SMS-сервера (Systems Management Server — сервер управления системами), поскольку он просто более надежен и предоставляет больше возможностей.

Утилита Network Monitor состоит из двух компонентов: инструментальных средств администрирования (Network Monitor) и сетевого протокола (Network Monitor driver). Чтобы анализировать кадры, вам необходимо установить оба компонента. Поэтому для удобства при установке Network Monitor вместе с ним автоматически устанавливается и драйвер. Это очень любезно со стороны Microsoft.

При установке Windows Server 2003 NetMon автоматически не устанавливается. Это служба, которую вам придется установить отдельно с помощью системной папки Control Panel. Чтобы установить NetMon на сервере, выполните следующие действия.

1. **Выберите команду Start⇨Control Panel⇨Add or Remove Programs (Пуск⇨Панель управления⇨Установка и удаление программ).**

   Появится диалоговое окно Add or Remove Programs.

2. **Щелкните на кнопке Add/Remove Windows Components (Добавление и удаление компонентов Windows).**

   Появится окно мастера Windows Components Wizard.

3. **Выберите пункт меню Management and Monitoring Tools (Программы управления и мониторинга) и щелкните на кнопке Details (Подробности).**

4. **В окне Management and Monitoring Toots установите флажок Network Monitor Tools (Программы мониторинга сети), а затем щелкните на кнопке OK.**

5. **Щелкните на кнопке Next** (Далее).

6. **Если мастер установки запросит у вас дополнительные файлы, чтобы завершить установку, выполните одно из следующих действий:**

   а) если вы копируете компакт-диск Windows Server 2003 в сеть, укажите мастеру путь к файлам;

   б) в противном случае вставьте компакт-диск Windows Server 2003 в устройство чтения компакт-дисков.

После того как все компоненты будут установлены, запустите утилиту NetMon из раздела Administrative Tools (Start⇨Administrative Tools⇨ Network Monitor (Пуск⇨Администрирование⇨Network Monitor)). Диалоговое окно на вашем экране должно выглядеть так, как на рис. 20.3.

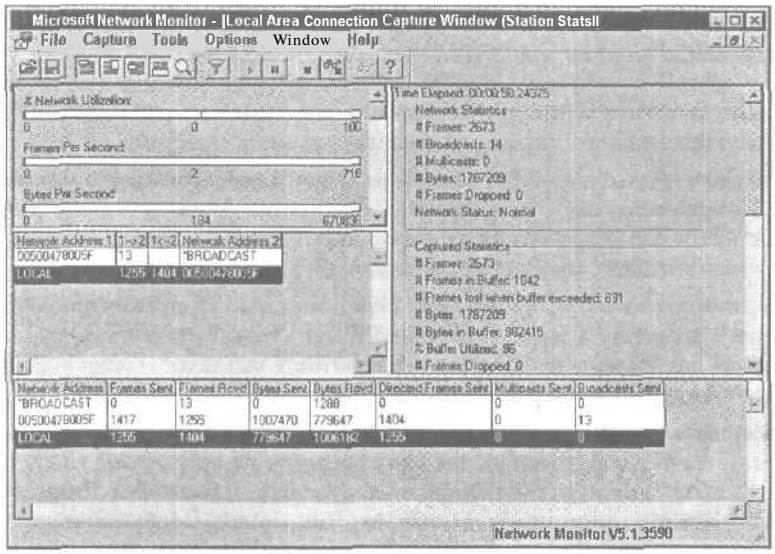


Рис. 20.3. Утилита Network Monitor в действии

После запуска утилиты NetMon можете установить фильтры для сбора только определенной информации. Например, вам не требуется отслеживать многоадресную информацию NetBIOS, но вам необходимо получить информацию, относящуюся к IP-протоколу. Вы устанавливаете фильтры, чтобы отделить необходимую информацию от лишней.

Вы можете "посадить" на события триггеры, действующие по принципу "если произойдет это, действуйте следующим образом". Например, если вы не желаете фиксировать все входящие и исходящие данные сервера, можете отслеживать определенную последовательность событий и, когда она наступит, собирать информацию. Эти отфильтрованные кадры помогут вам в дальнейшем уточнить, что вы наблюдаете в последовательности кадров.

Microsoft в избытке предоставляет информацию, касающуюся утилиты NetMon, с которой можно ознакомиться с помощью команды Start⇨Help and Support⇨Administration and Scripting Tools⇨Monitoring and Status Tools⇨Network Monitor (Пуск⇨Справка и поддержка⇨Администрирование и сценарии⇨Программы мониторинга и статуса⇨Сетевой монитор). Чтобы понять, что Microsoft считает лучшим способом установления в сети определенной функции, всегда начинайте с раздела Best Practices (Лучшие практики).

Проверьте сетевые установки еще раз!

Существует много причин, связанных с неверной настройкой конфигурации и изменениями, которые могут повлиять на работу сети. Приведенный ниже список вопросов поможет вам разобраться в положении вещей, которое, возможно, требуется изменить.

- ✓ **Верно ли настроены адреса (нет ли дублирования адресов)?** Каждый узел сети (включая серверы) должен обладать уникальным адресом и именем компьютера. Если у вас не получается выполнить процедуру PING (о программе PING см. в главе 14) или увидеть компьютер посредством броузера или Active Directory, убедитесь в корректности идентификаторов компьютера.
- ✓ **Верно ли установлены IP-диапазоны?** Если вы используете внутреннюю схему IP-нумерации, а затем подключаетесь к Internet, ваша схема может прийти в противоречие с другим зарегистрированным набором номеров. Прежде чем подключиться к Internet, свяжитесь с вашим поставщиком услуг Internet, чтобы удостовериться, что вы не установили сеть, воспользовавшись чужими IP-номерами.
- ✓ **Функционируют ли службы на сервере?** Иногда необходимая вам служба прекращает функционировать на сервере. Выберите команду Start⇨Administrative Tools⇨Services (Пуск⇨Администрирование⇨Службы) и проверьте, что служба установлена и запущена. Иногда вам необходимо будет запускать и останавливать службу.
- ✓ **Зарегистрированы ли какие-либо ошибки утилитой просмотра событий Event Viewer?** Загляните в журналы утилиты Event Viewer, чтобы проверить, зарегистрированы ли какие-либо ошибки (Start⇨Administrative Tools⇨ Event Viewer (Пуск⇨Администрирование⇨Просмотр событий)).
- ✓ **Существуют ли конфликты между устройствами?** Чтобы проверить, не конфликтуют ли между собой устройства из-за запросов на прерывания (IRQ) или памяти, используйте утилиту Conflicts/Sharing Manager. (Start⇨All Programs⇨System Tools⇨System Information⇨Hardware Resources⇨Conflict/Sharing (Пуск⇨Все программы⇨Служебные⇨Сведения о системе⇨Ресурсы аппаратуры Конфликты/Доступ). Вы можете также обратиться к утилите Device Manager, чтобы получить дополнительную информацию из этой же области.

- ✓ **Доступны ли соответствующие домены?** Убедитесь в наличии для сервера установленного и функционирующего контроллера домена, а также в доступности службы Active Directory.
- ✓ **Правильно ли присвоены права доступа?** Убедитесь в том, что пользователи обладают надлежащими правами в отношении групп и ресурсов, доступ к которым им необходим.
- ✓ **Верно ли установлены совместно используемые ресурсы?** Проверьте, что рассматриваемый ресурс обладает общедоступным статусом на сервере и представлен в Active Directory для всех или части пользователей. Иногда устройства не отображаются, потому что о них никто не знает.

Сервер недоступен

Когда пользователи не могут обнаружить сервер со своей рабочей станции, они начинают беспокоиться. Если только один пользователь не может обнаружить сервер, причина, вероятно, кроется в его рабочей станции. Если несколько пользователей не могут обнаружить сервер, вы, вероятно, столкнулись с проблемой сегмента, например отказал мост или маршрутизатор. (Более подробно о мостах и маршрутизаторах см. в главе 4.)

Если проблемы возникли у одного **пользователя,** ответьте на следующие **вопросы.**

- ✓ **Зарегистрировался ли пользователь в системе?** Не смейтесь, но иногда пользователи сообщают вам о том, что службы не работают, а сами не вошли в систему.
- ✓ **Работал ли пользователь с сетью прежде?** Если это новый пользователь, который входит в систему впервые, учетная запись может быть не установлена. Однако если пользователь недавно переведен из другого отдела, вам может потребоваться переназначить его в другую группу либо изменить его политику учетной записи.
- ✓ **Пытался ли пользователь перезагрузить рабочую станцию?** Иногда, если пользователь перезагружает свою рабочую станцию единовременная проблема исчезает.
- ✓ **Обладает ли пользователь надлежащими правами?** Проверьте политику учетной записи пользователя и разрешения и убедитесь, что он обладает надлежащими правами доступа к сети или каталогу, чтобы обратиться к необходимому ресурсу.
- ✓ **Вносил ли кто-то изменения в конфигурацию рабочей станции?** Если к рабочей станции были добавлены какие-либо устройства, запрос на прерывание (IRQ) нового устройства может конфликтовать с запросами на прерывание других устройств или является источником проблем с адресами памяти. Обратитесь к корневому каталогу рабочей станции и отсортируйте файлы по дате и времени, чтобы понять, когда были внесены последние изменения. Затем проверьте каталог Windows и отыщите файлы *.ini, чтобы выяснить, были ли внесены изменения в какой-либо из этих файлов. Если была добавлена новая сетевая плата, проверьте, настроена ли она на соответствующую скорость сети.
- ✓ **Можете ли вы "прозвонить" рабочую станцию пользователя?** Если на рабочей станции установлен протокол TCP/IP, попробуйте "прозвонить" рабочую станцию с помощью программы PING с вашей настольной системы, попробуйте "прозвонить" сервер с рабочей станции пользователя и попытайтесь обнаружить сервер в перечне сетевых ресурсов броузера или каталога. (Более подробно о программе PING см. в главе 14.) Если вам удается "прозвонить" сервер, но вы не видите сервер среди сетевых ресурсов в окне броузера, можно прибегнуть к выбору броузера в сети, чтобы переустановить основной броузер. Информация о выборе броузера содержится в документации TechNet (`www.microsoft.com/technet/`).

- ✓ **Не отказал ли стыковочный кабель?** Стыковочный (или "глянцевый") кабель — это серебристый кабель, иногда используемый для сетевого соединения между сетевым адаптером и настенной платой. Иногда во время уборки помещений пылесосы переезжают через кабель и повреждают его. Если кабель неисправен, вы можете легко заменить его. Если проблем с кабелем нет, проверьте сетевую плату. (Конечно, если это беспроводная рабочая станция, кабель не может быть причиной неисправности!)
- ✓ **Не отказал ли сетевой адаптер?** Иногда выходит из строя сетевой адаптер. Замените плату на заведомо рабочую, чтобы узнать, решит ли это проблему.

Вам также может потребоваться проверить следующие параметры системы.

- ✓ **Ограничения времени входа в систему. Если** пользователь может входить в сеть только в определенное время, проверьте конфигурацию пользователя, чтобы убедиться в отсутствии ограничений.
- ✓ **Служба удаленного доступа (Remote Access Service — RAS).** Если недоступный сервер — это сервер службы удаленного доступа, вы должны наделить пользователей полномочиями наборного доступа для подключения к RAS-серверу, включив полномочия в учетную запись.
- ✓ **Протокол DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации хост-узла).** Если недоступный сервер — это DHCP-сервер, убедитесь в том, что служба DHCP установлена и функционирует. (Выберите команду Start⇨Administrative Tools⇨Computer Management (Пуск⇨Администрирование⇨Управление компьютером), а затем раскройте узел Services and Applications (Службы и приложения)). Если пользователи, работа которых зависит от службы DHCP, не смогут увидеть DHCP-сервер, они не смогут получить IP-адрес.

Замедление работы сетевых служб

Когда сетевые службы начинают замедлять свою работу, проблемы, определенно, не заставят себя ждать. Когда такое случается, возможно, почти исчерпалось дисковое пространство на сервере, поэтому необходимо реконфигурировать память, либо сетевая плата Token Ring вышла из строя и разорвала сетевое кольцо. Если сетевые адаптеры сервера не в состоянии справиться с огромным трафиком, подумайте о переходе на более производительную сетевую плату. Не используйте для сервера устаревшие 8-разрядные сетевые платы, как минимум следует использовать 32-разрядные.

Тихо! Я слышу маяк

Технология Token Ring — чудная вещь, потому что образует кольцо, по которому перемещаются данные. Когда в кольце происходит разрыв, данные движутся по U-образному пути. Пользователи, расположенные в нижней части этого пути, не замечают существенного замедления, а те, кто расположен в вершинах U-образного сети, наблюдают значительное замедление. Разрыв маркерного кольца обычно происходит, когда кабели не в порядке или один из сетевых адаптеров начинает генерировать маяк. (Генерация маяка (beaconing) — процесс выдачи компьютерам в сети кольцевой топологии сигнала (маяка) о том, что передача маркера прервана из-за серьезной ошибки. — *Прим. ред.)* Если вы используете неинтеллектуальные концентраторы или модули MAU (Multistation Access Unit — модуль множественного доступа), вам следует изолировать неисправную плату Token Ring или порт устройства MAU с помощью процесса исключения. Мы обычно брали все кольцо и отключали одно устройство MAU за раз, а затем один за другим отключали порты. Устаревшие модули MAU

фактически представляют собой реле, поэтому вам следует использовать специальные инструменты MAU для восстановления работы реле. В иных случаях вам необходимо будет заменить отказавший сетевой адаптер.

Что происходит с пропускной способностью

Вам следует проверить, не "поглощают" ли приложения, выполняемые на сервере, слишком большую часть пропускной способности. Приложения, "пожирающие" пропускную способность, часто встречаются в 10-мегабитовых средах Ethernet, которые отличаются высоким уровнем сетевой активности и приложениями баз данных. В некоторых слабо спроектированных приложениях баз данных, когда пользователь выполняет запрос к базе данных, на рабочую станцию пользователя загружается для обработки все содержимое базы данных. Это создает огромный дополнительный трафик. Чтобы сгладить эту проблему, вы можете перейти на ПО баз данных, которое обладает процессором баз данных, способным дробить записи; пользователи получают только результат. Другим решением этой проблемы является переход на более быструю сетевую схему, такую как 100-мегабитовая сеть Ethernet.

Большие объемы сетевой печати также могут привести к проблемам. Если некоторые пользователи или группы пользователей печатают в течение дня большие объемы данных, подумайте о том, чтобы перевести их на печать ночью (по возможности), чтобы устранить перегрузку сети. Вы можете установить такие параметры печати для этих пользователей, которые позволяют выводить на печать их информацию только в определенные часы.

Некоторые организации идут на замену существующих сетевых магистралей, чтобы избавиться от перегрузки пропускной способности, однако соответствующие затраты велики. Организации, которые располагают удаленными офисами, иногда размещают дополнительный сервер Windows Server 2003 в удаленном офисе и устанавливают его как контроллер домена. Это позволяет идентифицировать пользователей локально в удаленном офисе и сберечь, таким образом, пропускную способность глобальной сети. Другие организации выбирают вариант обновления существующей сетевой магистрали до 100 Мбит/с, в то время как пользователи по-прежнему подключены к концентраторам со скоростью 10 Мбит/с. Это связано с обновлением устройств, подключенных к магистрали, чтобы перейти на 100-мегабитовые сетевые адаптеры и кабели, а также добавлением переключателя, который может работать как со скоростью рабочей станции в 10 Мбит/с, так и со скоростью сетевой магистрали в 100 Мбит/с. При такой переделке, даже если пользователи работают на всю мощь, 90 процентов пропускной способности сервера остается в распоряжении клиентов.

Конфликты в сети

Если вы работаете с сетью Ethernet, в которой наблюдается множество конфликтов и ошибок, может возникнуть проблема с методом доступа к среде CSMA/CD (Carrier Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением конфликтов). Если в вашей сети установлены интеллектуальные концентраторы, вы можете просматривать информацию о сети либо посредством графического интерфейса, либо наблюдая за светодиодами концентратора. Высокая частота конфликтов обычно служит индикатором отказавшей проводки или неисправных плат. Это может также означать высокий коэффициент использования пропускной способности. Сети Ethernet обладают более низким коэффициентом использования пропускной способности, чем сети Token Ring. Иногда вам понадобится разделить пользователей, которые инициируют высокие объемы сетевых обменов, на сегменты.

Куда девается дисковое пространство

Если дисковое пространство вашего сервера исчерпалось, вас ожидает целый "букет" проблем, поскольку на сервере могут храниться очереди печати, а также данные пользователей и приложений. Когда свободное дисковое пространство начинает уменьшаться, появляется масса странных проблем. Вы должны приобретать оперативную память с запасом, поскольку Windows 2003 использует значительно больший объем памяти, чем ее предшественница, Windows NT. Если в вашем распоряжении имеется только минимум памяти, рекомендуемый Microsoft, при попытке выполнить больше одной задачи вы столкнетесь с проблемами, так что добавьте объем памяти, значительно превышающий минимум.

Windows 2003 использует дисковую память для подкачки информации в оперативную память и обратно. Поэтому чем больше объем оперативной памяти вашей системы, тем быстрее осуществляется доступ к файлам. Вы можете получить информацию о памяти вашей системы и ее использовании с помощью команды Start⇨All Programs⇨Accessories⇨System Tools⇨System Information⇨System Summary (Пуск⇨Программы⇨Стандартные⇨Служебные⇨Сведения о системе⇨Сведения о системе).

V При недостатке дискового пространства Windows 2003 испытывает трудности при попытке записи в файл `Pagefile.sys`. Чтобы получить информацию об этом файле и изменении его минимального и максимального объема, выберите команду Start⇨Control Panel⇨System (Пуск⇨Панель управления⇨Система), щелкните на вкладке Advanced (Дополнительно), а затем щелкните на кнопке Settings (Параметры) в разделе Performance (Производительность). В появившемся окне Performance Options (Параметры производительности) щелкните на вкладке Advanced (Дополнительно), а затем щелкните на кнопке Change (Изменить) в разделе Virtual Memory (Виртуальная память). На экране отобразится диалоговое окно, показанное на рис. 20.4.

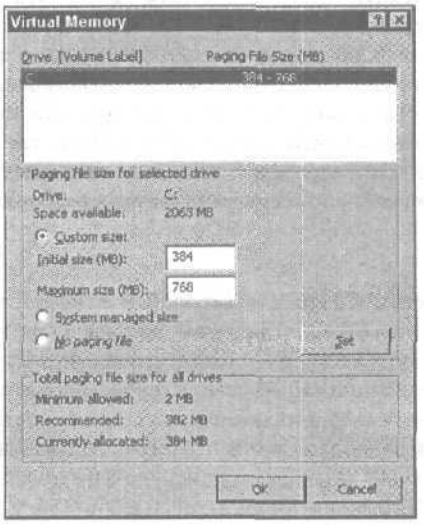


Рис. 20.4. Диалоговое окно VirtualMemory

Вам необходимо установить по меньшей мере минимальное и максимальное значения, рекомендуемые системой Windows 2003.

Задачи, которые лучше выполнять в нерабочее время

Приходилось ли вам выполнять сетевую задачу по пересылке большого объема данных, например, связанную с восстановлением большого количества файлов? Или приходилось ли восстанавливать синхронизацию зеркальных дисков? Если в сети имеются устройства большой емкости, которые дублируют информацию друг друга (так называемые "зеркальные" диски), и их синхронизация нарушается, вы можете се восстановить, но выполнять подобную задачу в рабочее время не стоит. Проверьте, осуществляет ли кто-нибудь некоторый вид поддержки — в сети или на сервере. Если необходимо выполнить крупномасштабное восстановление файлов посредством сети, попробуйте сделать это в периоды ее наименьшей загрузки.

Если вы обратились к системному монитору (System Monitor) и обнаружили большую загруженность ресурсов, вы можете выяснить, что является источником подобной проблемы, выбрав команду Start⇨Administrative Tools⇨Computer Management (Пуск⇨Администрирование⇨ Управление компьютером). Затем, раскрыв узел System Tools⇨Shared Resources (Служебные программы⇨Общие папки), вы можете проверить использование ресурсов применительно к отдельным системным папкам и пользователям.

Когда нельзя попасть "отсюда" "туда"

Когда сегмент сети выходит из строя, становится невозможным попасть в определенную точку сети. Причиной подобной ситуации может быть несколько факторов, в зависимости от конфигурации вашей сети. Чтобы выяснить, что именно отказало, попробуйте "прозвонить" различные узлы сети с помощью программы PING. Например, если в результате выполнения программы PING вы получили отклик от одного из интерфейсов маршрутизатора и не получили ответа от остальных интерфейсов, проблема, вероятно, кроется в маршрутизаторе. Вы также можете воспользоваться таким средством, как TRACERT, применительно к протоколу TCP/IP (см. главу 14), чтобы определить время прохождения сигнала между текущим и конечным пунктами назначения. Медленное прохождение сигнала между двумя пунктами назначения может указывать на точное место возникновения проблемы. Чтобы более точно определить, что можно увидеть из разных пунктов сети, попробуйте использовать инструменты PING и TRACERT в различных точках сети.

Чтобы определить вероятное место отказа сети, используйте больше одной утилиты. Например, утилита PING работает только с протоколом TCP/IP. Попробуйте использовать другую утилиту, например NBTSTAT, которая работает с протоколами NetBIOS и TCP/IP.

Препятствовать вашему доступу к сети могут также перечисленные ниже причины.

- ✓ Маршрутизатор. Маршрутизаторы соединяют разные сети. Если вы неверно определили маршрутизатор, вы не сможете увидеть, что находится "на другой стороне". Маршрутизаторы могут также испытывать перегрузку и выбрасывать пакеты данных. В этих случаях вам, возможно, необходимо увеличить память маршрутизатора. Устаревшие маршрутизаторы также требуют замены микросхем; модификация более новых маршрутизаторов может сводиться к перепрограммированию существующих микросхем. Проверьте, какую версию ПО использует ваш маршрутизатор, и обратитесь к фирме-изготовителю.
- ✓ Моет. Если ваша сеть содержит мосты, иногда вам понадобится перезагрузить мост. Это может случаться и часто, в зависимости от используемого программного и аппаратного обеспечения. Помните, что мосты требуют высококачественных сетевых адаптеров, поскольку они передают огромное количество пакетов между мостами. (Более подробно о мостах см. в главе 4.)

- ✓ **Глобальные каналы.** В случае отказа канала T1 или канала с пропускной способностью 56 Кбит вы не увидите ничего по другую сторону канала. Иногда для решения этой проблемы вам может потребоваться вызвать представителей телекоммуникационной компании. Вам необходимо иметь под рукой информацию о канале и номер телефона службы поддержки клиентов.
- ✓ **Концентратор.** Если вы утратили целый сегмент сети, проверьте концентратор, который соединяет этот сегмент. Концентраторы обычно снабжены источником питания и портами, которые могут выйти из строя. Иногда простого подключения узла к другому порту бывает достаточно, чтобы устранить неисправность. Обязательно обозначьте порт как неисправный, чтобы кто-то другой не подключил устройство к этому порту (например, обведите его кружком).
- ✓ **Кабельная система.** Со временем кабельная система приходит в негодность, либо кабели перекладываются с места на место, что в конце концов может служить причиной их разрыва. Чтобы проверить, исправны ли кабели, воспользуйтесь утилитой TDR (Time-Domain Reflectometer — динамический рефлектометр). Возможно, вам потребуется протянуть новый кабель к настольной системе или серверу. Если вы подозреваете, что уборщики прошлись пылесосом по одному из ваших соединительных кабелей и повредили его, замените кабель!
- ✓ **Сервер.** Проверьте, что данный сервер включен и функционирует. Это кажется очевидным, но в любом случае проверьте его.
- ✓ **Разрешение имен.** Вам может потребоваться установить службу WINS (Windows Internet Naming Service — служба имен Internet для Windows), DHCP или хост-файл в зависимости от протоколов, используемых в вашей сети. (Более подробно о протоколах TCP/IP см. в главе 14.)

Выявление нерегулярных проблем

Нерегулярные или перемежающиеся проблемы намного более трудны для разрешения, поскольку не проявляются по вашему желанию и вы не всегда в состоянии воспроизвести их. Проблемы этого типа возникают в результате последовательности событий, обычно следующих в определенном порядке, который вам неизвестен. Ваша задача состоит в том, чтобы установить последовательность событий. Вы скажете: "Это невозможно!" Ничего подобного!

Если вы начали процедуру входа в систему, зафиксируйте следующие моменты, которые помогут вам исключить возможные причины проблем.

- ✓ **Заметьте время и дату возникновения проблемы.** Например, проявляется ли проблема только в 10 часов утра по четвергам? Возможно, некоторая ситуация в одном из подразделений повторяется каждую неделю, например перед совещанием отдела, когда все пытаются получить доступ к сети или напечатать отчет. Высокая активность пользователей может создать перегрузку для сервера или сети. Понаблюдайте за тенденциями в датах и во времени. В случае подобных подозрений используйте утилиту System Monitor.
- ✓ **Зафиксируйте используемое оборудование.** Проявляется ли проблема только для определенного сервера или рабочей станции? Возникает ли проблема только при входе определенного пользователя в сеть? Проверьте информацию учетной записи пользователя, а также его файлы конфигурации.

- **Зафиксируйте используемые приложения.** Проявляется ли проблема только при использовании определенного приложения? Переустановите приложение. Файл приложения может быть поврежден, и это повреждение может быть незамечено до тех пор, пока пользователь не выполнит определенную функцию этого приложения.
- **Зафиксируйте используемую среду.** Проявляется ли проблема только на определенном этаже, вблизи некоторого участка, например лифта? Если это так, возможно, возникли помехи в кабелях вблизи мощного оборудования или флуоресцентного освещения.
- **Проверьте журнал посещений.** Проявляется ли проблема всякий раз, когда работник службы поддержки открывает кабельный шкаф или входит в машинный зал? Если это так, проследите за этим человеком в следующий раз и посмотрите, что он делает. (Не забудьте про плащ и темные очки!)
- **Вирусы.** Вирусы представляют собой одну из самых очевидных причин возникновения проблем, поэтому, наверное, о них вспоминают в последнюю очередь. Вирусы служат причиной странных явлений в сети. Если у вас появились подозрения в отношении вирусов, немедленно отключите сервер от локальной и глобальной сети и просканируйте его. До последнего времени этого было достаточно. Не забудьте предупредить ваших пользователей, чтобы они не отправляли электронные сообщения при подозрении на вирус. Вам, возможно, придется отключить почтовый сервер компании, чтобы гарантировать, что в это время никакая электронная почта не распространяется.
- **Известные дефекты.** Иногда вы бьетесь головой о стену, пытаясь разрешить проблему, которая в действительности является известным дефектом. Регулярно обращайтесь на Web-узел Microsoft и следите за появлением новых пакетов обновления. Также не забывайте посещать Web-узлы других организаций. Например, если вы используете пакет Microsoft Office, проверьте, не появились ли на Web-узле Microsoft пакеты обновления для него. Если вы используете сетевые карты 3Com Ethernet, посетите Web-узел компании 3Com и узнайте, не появились ли обновления для драйверов с исправленными ошибками. Если вы будете в курсе известных проблем, это сэкономит вам время.

Глава 21

Восстановление работы Active Directory

В этой главе...

Служба Active Directory — жизненно важная часть Windows Server 2003. Как уже говорилось в главах 11 и 12, Active Directory управляет всеми важными сетевыми объектами. Какие объекты имеются в виду? Это — учетные записи пользователей, общие (сетевые) ресурсы, разрешения на доступ к компьютеру и элементы управления политикой групп.

Когда компания Microsoft разрабатывала Active Directory, она отдавала себе отчет в том, что любые проблемы, возникающие с этой базовой службой, могут привести к проблемам во всей сети. Поэтому она обеспечила высокую отказоустойчивость службы Active Directory, снабдив ее определенными механизмами, которые помогают Windows Server 2003 надежно выполнять свои повседневные функции. В этой главе мы расскажем об этих возможностях восстановления Active Directory Windows 2003.

Отказоустойчивая система (fault-tolerance system) — это система, которая может сохранять работоспособность при возникновении программных или аппаратных ошибок. Кроме того, отказоустойчивость препятствует потере данных.

Самовосстановление контроллера домена

Active Directory обладает способностью к динамическому самовосстановлению или, по меньшей мере, самообслуживанию. Служба Active Directory выполняет регулярные самопроверки на предмет внутренней непротиворечивости и потери данных, а также на наличие элементов, утративших актуальность. По умолчанию операция "сборки мусора" выполняется каждые 12 часов и состоит в удалении журналов, элементов, срок действия которых истек, и дефрагментации файла базы данных. Журналы, удаляемые в ходе операции "сборки мусора", относятся к журналам регистрации изменений или транзакций, которые временно хранят операции. После того как система проверит, что все действия, записанные в эти журналы, успешно выполнены, журналы удаляются, поскольку необходимость в них отпадает.

Данные на жестком диске подвергаются естественной фрагментации (или расщеплению), что приводит к замедлению доступа к данным. Процесс реорганизации данных для приведения их в порядок и максимизации производительности называется *дефрагментацией (defragmentation)*.

По мере того как Active Directory изменяется и приспосабливается к сетевой среде, отношения и другие связанные с объектами данные устаревают. Эти данные вместе с удаленными элементами, которые все еще остаются в базе данных, удаляются. С помощью дефрагмента-

ции файла базы данных данные располагаются компактно, а файл переупорядочивается, что способствует повышению производительности.

Когда дефрагментация выполняется системой, она называется *оперативной дефрагментацией (online defragmentation)*. Оперативная дефрагментация создает свободное пространство внутри существующего файла базы данных для новых элементов, однако она не возвращает пространство файловой системе для использования другими файлами. Только автономная дефрагментация возвращает неиспользуемое пространство базы данных файловой системе. Microsoft рекомендует выполнять автономную дефрагментацию только в случае крайней необходимости (например, когда отсутствует достаточный объем доступной дисковой памяти для выполнения обычных системных операций). Для запуска автономной дефрагментации перезагрузите систему и нажмите клавишу <F8>, чтобы получить доступ к загрузочному меню. Затем выберите пункт меню Directory Services Restore Mode (Режим восстановления службы каталогов), с помощью которого выполняется процедура автономной дефрагментации загрузки системы в безопасном режиме. Вам необходимо будет вновь перезагрузить систему, чтобы вернуться к полнофункциональному режиму работы с сетевой поддержкой.

Нарушения в работе Active Directory

Иногда ошибки администраторов приводят к проблемам, отказ сетевого соединения препятствует доступу к данным, либо блуждающее нейтрино выбивает элемент данных в файле базы данных. В любом случае необходимо исправить ситуацию, чтобы восстановить нормальную работу Active Directory.

Справочная система Windows 2003 (Help and Support System) предоставляет возможности выявления и устранения проблем Active Directory в форме проблемно-ориентированных сценариев, содержащих детализированное описание причин возникновения проблем и их решений. Мы обнаружили, что эта информация чрезвычайно полезна при решении практически любых проблем Active Directory, с которыми мы сталкивались. Чтобы получить доступ к информации, связанной с проблемами Active Directory, выполните следующие действия.

1. **Выберите команду Start⇨Help and Support (Пуск⇨Справка и поддержка).**

   Появится диалоговое окно Help and Support Center Windows 2003.

2. **В списке, размещенном в левой части окна, выберите элемент Active Directory, щелкните на подпункте Troubleshooting, а затем на элементе Troubleshooting Active Directory.**

   В правой панели отобразится список возможных проблем Windows 2003.

3. **В правой панели щелкните на названии темы, которая наиболее подходит к вашей ситуации.**

   При открытии списка отобразится детализированное описание причин проблем и возможных решений. Возможно, вы обнаружите, что для восстановления вашей системы требуется внести небольшие исправления.

Распространенные проблемы

Раздел выявления и устранения проблем для Active Directory службы Help and Support Center может указать вам кратчайший путь к решению проблем. Однако вы можете попробовать отыскать свой собственный путь к решению проблемы без всяких подсказок. К счастью для вас, наиболее распространенные проблемы, которые являются результатом отказов или неверных действий Active Directory, относительно легко обнаружить.

Нарушение взаимодействия

Наиболее распространенной проблемой Active Directory является нарушение взаимодействия. Попросту говоря, все, что препятствует четкой и полной передаче пакетов данных между двумя сетевыми хост-узлами, можно отнести к нарушению взаимодействия. Причины подобного рода нарушений могут быть весьма просты, например разрыв сетевого кабеля или неподключенный к сети компьютер. Более сложные проблемы, такие как маршрутизатор с разрушенной таблицей маршрутизации или DNS-сервер с неверно определенными записями, также могут стать причиной нарушения взаимодействия. Если проблема носит физический характер, вам может потребоваться заменить кабель или перезагрузить систему для восстановления ее функционирования. Если проблема более сложная, вам необходимо исследовать возможности устранения проблемы применительно к специфике конкретной службы Windows 2003.

Если вы *подозреваете*, что произошло нарушение взаимодействия, можете воспользоваться обычными сетевыми инструментами, чтобы получить конкретную информацию. Например, если ваша сеть использует протокол TCP/IP, вы можете воспользоваться средствами, разработанными для выявления и устранения проблем, связанных с этим протоколом. Два наиболее полезных инструмента для работы с этим протоколом — утилиты PING и TRACERT. (Более подробно о программах PING и TRACERT см. в главе 14.) Утилита PING информирует вас о том, могут ли пакеты данных проходить по сети от вашей системы к любому другому хост-узлу. Утилита TRACERT информирует о каждом отрезке сетевого пути между маршрутизаторами от вашего до любого другого хост-узла, а также о том, невозможна ли передача данных после определенной точки сетевого маршрута.

Если результат выполнения утилит PING и TRACERT показывает, что пакеты данных даже не выходят за пределы вашего компьютера, для проверки правильности установки протокола TCP/IP на вашем компьютере и корректности настройки параметров этого протокола (IP-адрес, маска подсети, шлюз по умолчанию и т.д.) используйте команду `IPCONFIG/ALL`. Если какие-либо параметры выбраны неверно, измените их с помощью интерфейса Local Area Connection (Локальное соединение) (Start⇨Control Panel⇨Network Connections (Пуск⇨Панель управления⇨Сетевые соединения)) и перезагрузите систему.

Проблемы политик групп

Еще одна распространенная проблема возникает вследствие применения политик групп, которые либо слишком ограничивают доступ, либо противоречат или перекрывают друг друга, что приводит к противоречиям в функционировании системы, Вам необходимо проверить политики групп для каждого домена, пользователя, группы и производственного подразделения, чтобы определить источник проблемы.

Взаимодействие контроллеров домена

Если взаимодействие резервных контроллеров доменов Windows NT 4.0 и контроллеров доменов Windows Server 2003 не разрешено, вы, вероятно, включили собственный режим работы. Служба Active Directory Windows Server 2003 может работать в четырех режимах: смешанном режиме Windows 2000, собственном режиме Windows 2000, режиме Windows .NET и промежуточном режиме Windows .NET.

Смешанный режим Windows 2000 используется по умолчанию и позволяет взаимодействовать контроллерам доменов Windows Server 2003 и контроллерам доменов Windows NT 4.0 Server, установленным в качестве резервных контроллеров доменов (BDC-контроллеров). *Собственный режим Windows 2000* препятствует участию серверов Windows NT 4.0 в управлении доменами.

Большая проблема с параметрами режима состоит в том, что, после того как они установлены в собственный режим, их нельзя вернуть назад без полной переустановки системы. Поэтому администраторы должны переключать домены в собственный режим только в случае абсолютной уверенности в том, что BDC-контроллеры Windows NT 4.0 больше не потребуются.

Установка режима осуществляется с помощью утилиты Active Directory Domains and Trusts (Домены и доверенности Active Directory). Выберите домен, режим работы которого вы намерены переключить, а затем выберите команду Raise Domain Functionality (Повысить функциональность домена). После этого в диалоговом окне Raise Domain Functionality выберите функциональный уровень (режим) из списка Select an Available Domain Functional Level (Выбор подходящего функционального уровня домена).

Если сочетание процедуры автоматизированной "сборки мусора", инструкций справочной системы Windows 2003 и ваших собственных усилий по поиску и устранению проблемы не позволило устранить проблемы с Active Directory, остается только одно решение — восстановление резервной копии.

Создание резервной копии и восстановление данных каталога

Для восстановления Active Directory из резервной копии требуется одна очень важная вещь: своевременно созданная резервная копия системы. Без последней резервной копии системы, созданной во время ее нормального функционирования, вы не сможете восстановить Active Directory.

Подготовка восстановления Active Directory с использованием резервной копии требует наличия полной резервной копии всей системы. Это означает создание резервной копии с помощью мастера резервного копирования (Backup Wizard) и выбора опции Back Up Everything on My Computer (см. главу 17). При наличии резервной копии восстановить систему не трудно.

1. **Переустановите Windows Server 2003.**

   Убедитесь в том, что при установке системы используются те же имена разделов и корневого каталога, что и раньше.

2. **Используйте утилиту Backup для восстановления всех данных из резервной копии в их первоначальное состояние.**

3. **Завершив восстановление, перезагрузите систему.**

   Windows Server 2003 автоматически распознает, что она восстановлена из резервной копии, и перестраивает базу данных Active Directory.

Итак, единственным средством для восстановления серьезно поврежденной системы является своевременное и полное резервирование. Как мы подчеркивали в главе 17, вам необходимо внедрить регулярную жестко регламентированную процедуру резервирования, чтобы защитить свои данные.

Если вы желаете получить больше информации о том, как справиться с проблемами Active Directory, обратитесь к справочной системе Windows Server 2003 (Help and Support Center), к документации Windows Server 2003 Resource Kit и TechNet (www.microsoft.com/technet/).

Часть VI

Великолепные десятки

"Веди машину осторожно, не забывай пообедать и всегда делай резервную копию твоего дерева каталогов перед изменением файла разбиения жесткого диска".

В этой части...

Когда Моисей спустился с горы, сколько заповедей он принес? Десять. Сколько пальцев на руках у людей? Десять. Какой балл самый высокий в десятибалльной системе? Десять. Мы не уверены полностью, что между всеми этими фактами существует связь, но рискнем утверждать, что "Великолепные десятки" — ключевой компонент этой и других книг серии *...для "чайников"*. Хотя все это, конечно, может быть простым совпадением.

Каждая глава этой части включает перечень советов, приемов, напоминаний и источников информации, касающейся системы Windows Server 2003 и созданных на ее основе сетей. Мы хотели бы претендовать на тот же источник вдохновения, который послужил Моисею для его заповедей, но "Великолепные десятки" являются всего лишь результатом нашего тяжкого опыта.

Эти главы построены так, чтобы сберечь ваше время и избежать распространенных ловушек.

Глава 22

Десять советов по установке и конфигурированию Windows Server 2003

В этой главе...

- Реальные требования Windows Server 2003
- Предварительная проверка оборудования
- Установка Windows 2003 с использованием сети
- Автоматизация установки
- Устранение проблем установки
- Использование режима VGA
- Возврат к прежней конфигурации
- Использование загрузочного компакт-диска
- Принятие предупредительных мер
- Планирование успешной установки сервера

Если вы уделяете довольно много времени работе с Windows Server 2003, от вас бесспорно потребуется установить это ПО на нескольких системах. Эта задача может быть более "интересной", чем следует, — не говоря уж о том, что она может занять больше времени, чем вы желали бы ей посвятить.

Эта глава указывает на некоторые полезные источники информации, включает хорошо зарекомендовавшие себя на практике правила и некоторые великолепные инструменты и методы, которые помогут вам успешно пережить процесс установки Windows Server 2003. Знать эти советы и не нуждаться в них — лучше, чем не знать и нуждаться.

Реальные, а не минимальные требования

В табл. 22.1 содержится краткий перечень минимальных требований к функционированию Windows Server 2003 (а вдобавок — реальные требования).

Конфигурация производственного сервера, которая просто удовлетворяет минимальным требованиям, — прямой путь к катастрофе. Продуктивность (или отсутствие оной), которую вы сможете выжать из подобной машины, обеспечит вам толпы пользователей, бесконечно преследующих вас по пятам.

При сборке компьютера Windows Server 2003 справедлив принцип: чем больше, тем лучше. Это относится к более мощному (и большему количеству) ЦП, большему объему ОП и более мощным платам сетевого интерфейса. Большую часть своих дел серверы вершат в "темноте", так что вам нет необходимости устанавливать графический адаптер с 16 Мбайт

памяти, невообразимый монитор, или дорогостоящую мышь, или сенсорную панель. У вас есть возможность игнорировать отсутствие на компьютере Windows Server 2003 компакт-диска или DVD до тех пор, пока вы можете получать доступ к серверу через сеть с другой машины, на которой содержимое компакт-диска скопировано на жесткий диск.

Таблица 22.1. Минимальные и реальные требования к Windows Server 2003

Элемент	Минимальные требования	Реальные требования
Компакт-диск	**Отсутствуют**	**Накопитель CD-ROM (12x или выше) или** DVD
Процессор	Pentium 133 МГц	Pentium 550 Мгц и выше
Дисковая память	Свыше 1,5 Гбайт	4 Гбайт и больше
Дисплей	VGA	SVGA с разрешением **800x600** и **выше**
Флоппи-диск	3,5 дюйма (необязательно)	3,5 дюйма
Сетевой адаптер	**По меньшей** мере **один**	Сетевой адаптер, управляемый шиной PCI (по меньшей **мере** 32-разрядный)
Указательное устройство	MS-мышь или совместимая (необязательно)	MS-мышь
Оперативная память	128 Мбайт или больше	256 Мбайт и больше (максимум — 4 **Гбайт)**

Если вы устанавливаете Windows Server 2003 на машине, на которой отсутствует сетевой адаптер, вы не сможете установить или настроить конфигурацию ни на одной из его сетевых функций. Мы убеждены, что устанавливать сервер на машину, которая не подключена к сети, не имеет смысла, так что не устанавливайте Windows Server 2003 на машине, пока она не снабжена сетевой платой (еще лучше, если адаптер подключен к реальной, действующей сети).

Используйте только подходящее серверное оборудование

Прежде чем вы даже подумаете об установке Windows Server 2003 на машине, вы должны быть совершенно уверены в том, что рассматриваемое вами оборудование наилучшим образом подойдет для этого программного обеспечения. Однако, как вы можете быть уверены, что ПО будет работать с приобретенным вами оборудованием, без формальных заверений или гарантий со стороны поставщика?

К счастью, вы можете обрести такую уверенность, сверившись с HCL-списком (Hardware Compatibility List — список совместимого оборудования). Это исчерпывающий перечень оборудования, которое было испытано и сертифицировано на совместимость с системами Windows 2003. Получить доступ к HCL-списку можно, обратившись на Web-узел `www.microsoft.com/hcl/`.

Вы можете также использовать утилиту для автоматической проверки оборудования. Однако для использования последнего доступного HCL-списка система должна иметь доступ к Internet. Существуют два способа испытать систему на HCL-совместимость. Первый заключается в том, чтобы вставить компакт-диск и включить механизм автозапуска (либо выполнить команду `startup.exe` из корневого каталога компакт-диска). Щелкните на кнопке Check System Compatibility (Проверить совместимость системы), а затем выберите опцию

Check My System Automatically (Автоматическая проверка системы). Второй способ заключается в выполнении следующей команды из приглашения для ввода командной строки или диалогового окна Run (Выполнить):

```
I386\winnt32 /checkupgradeonly
```

В обоих случаях пытаются вначале загрузить последний HCL-список, а затем испытать аппаратное обеспечение системы на совместимость с требованиями для Windows 2003. При обнаружении какой-либо проблемы или несовместимости на экране отобразится соответствующее сообщение,

Многие поставщики оборудования предлагают серверные машины с предустановленной системой Windows Server 2003. При покупке нового сервера приценитесь к машине, которая включает операционную систему Windows Server 2003, и к той, которая не включает ее. Вы будете приятно удивлены тем выигрышем, который получите при покупке предустановленной системы.

Установка Windows Sewer 2003 с помощью сети

Следующее утверждение может противоречить здравому смыслу, но это так и есть: копирование файлов с жесткого диска, расположенного где-либо в сети, осуществляется быстрее, чем копирование файлов с локального компакт-диска (даже для 36- или 40-скоростного устройства чтения компакт-дисков). Почему? Потому что жесткий диск по-прежнему в 100 раз быстрее устройства чтения компакт-дисков.

Опытные сетевые администраторы создают набор каталогов на сетевом диске и устанавливают Windows Server 2003 по всей сети, где только могут. Эта тактика отличается быстротой, легкостью и требует только однократной загрузки компакт-диска, независимо от того, сколько раз вы осуществляете установку. Фактически сетевая установка делает возможной автоматизированную установку, речь о которой идет в следующем разделе.

Дайте ПО поработать: автоматизированная установка

Обычно пользователь вводит имена дисков для программы установки Windows 2003: в текстовом виде в строку приглашения на этапе первоначальной загрузки и с использованием системы навигации но меню на более поздних этапах. В качестве альтернативы установкой Windows 2003 могут управлять текстовые файлы вызова ответов, делая возможным более-менее полно автоматизировать установку. Установка, управляемая сценариями, может быть особенно удобной, когда вы должны установить больше двух или трех копий Windows Server 2003 в любое заданное время.

Windows 2003 поддерживает больше способов автоматизации установки, чем предыдущие реализации (наподобие Windows NT), включая следующие.

- ✓ Новый [GuiRunOnce] раздел файла ответов, содержащий список команд для выполнения, когда пользователь входит в систему впервые после завершения "порции" установки в режиме GUI-интерфейса.

- ✓ Вы можете создать набор автоматических команд для завершения процесса установки, не требующих вмешательства человека (по крайней мере до тех пор, пока не встретятся какие-либо ошибки).
- ✓ Вы можете даже автоматизировать первый вход в систему после завершения установки Windows 2003 для установки и конфигурирования выбранных приложений, а затем соответственно остановить систему, и все это при помощи магических файлов ответов.

Как вам получить малую толику этого волшебства? Вы можете отыскать и отредактировать заранее определенный файл ответов под названием `unattend.txt` в документации Windows Server 2003 Resource Kit. Либо можете работать с утилитой Setup Manager, которую вы должны установить в системе после завершения базовой установки, чтобы создать файл с нуля. (Чтобы установить программу Setup Manager, выберите файл `Support\Tools\deploy.cab` на инсталляционном компакт-диске Windows Server 2003.)

Утилита Setup Manager аналогична утилите с таким же названием, работавшей под управлением Windows 98. Этот великолепный инструмент предоставляет в распоряжение пользователя кнопки, которые отображаются на разных этапах процесса инсталляции и проведут вас через диалоговые окна, чтобы задать сценарий для установки системы для единственного пользователя или нескольких систем одновременно.

Windows 2003 также включает две утилиты, которые в чем-то напоминают утилиту Ghost. (Ghost — популярная утилита представления системы для Windows NT 4.0, которая позволяет администраторам устанавливать единственную систему, делать "моментальный снимок", а затем настраивать его для установки систем на одной, двух и более машинах одновременно.) Вот эти две утилиты.

- ✓ Sysprep. Утилита, разработанная для дублирования содержимого диска при установке системы на нескольких одинаково сконфигурированных машинах одновременно. Сначала вы создаете обычную конфигурацию установки на одной машине, а затем устанавливаете приложение, которое намерены распространить. После этого вы используете Sysprep для распространения копий этой конфигурации на другие аналогичные системы в сети. Нет ничего проще!
- ✓ Syspart. Утилита, разработанная для "клонирования" инсталляций на нескольких машинах, оборудование которых отличается. Она работает как расширение неподдерживаемой функции установки с используемым по умолчанию файлом ответов `unattend.txt`.

Обратитесь к руководству Windows Server 2003 Resource Kit (опубликованному Microsoft Press) или компакт-диску TechNet, чтобы выяснить все, что возможно, о различных файлах инсталляции, прежде чем начинать любую большую работу. Вы также получите хороший совет выполнить два-три прогона с использованием этого средства, прежде чем предпринимать попытку автоматизировать установку на одном или нескольких производственных серверах.

Устранение проблем установки

Несмотря на все ваши усилия и предусмотрительность, изредка инсталляция Windows 2003 не выполняется. Мы были свидетелями различных случаев отказа: от неисправного носителя и перегрузки сети (при попытке скопировать файлы на слишком большое количество машин одновременно) до вирусов в загрузочном секторе (мы ненавидим подобную ситуацию!)

Когда инсталляция не выполняется, сделайте глубокий вдох, посчитайте до десяти и воспользуйтесь следующими советами.

- ✓ **Повторный запуск установки.** Если вы миновали начальную часть стадии текстового режима установки ПО, зачастую оказывается достаточно "сообразительным", чтобы указать вам, где оно "слетело", и продолжить с этого места. Если вам так повезло, благодарите судьбу, идите и без промедления купите лотерейный билет!
- ✓ **Если место отказа инсталляция неочевидно, загляните в каталог SWIN_NTS.~LS.** (Если вы выполняете установку без флоппи-диска с параметром /B, также загляните в каталог SWIN_NT$.~BS. Удалите один (или оба) из этих каталогов и их содержимое.) Программа установки Windows 2003 пытается найти эти каталоги и сохранить время, сообщая, в каком месте она "слетела". Этот метод хорош для корректных и чистых копий, но может не работать при возникновении проблем. Мы включили команду DOS DELTREE в наш инструментальный пакет диска аварийной инсталляции, поскольку он позволяет легко и быстро уничтожить эти каталоги.
- ✓ **Если отказ не устранен, выполните повторную разбивку на разделы форматирование загрузочного диска, чтобы удалить все следы неудачной инсталляции.** Вы начинаете с чистого листа! Наш инструментальный пакет диска аварийной инсталляции также включает команду DOS FDISK и удобную утилиту под названием Delpart.exe, которая может удалять даже разделы, отличные от разделов DOS (наподобие NTFS-разделов) с жесткого диска ПК. Утилиту Delpart.exe можно бесплатно загрузить с нескольких Web-узлов. Воспользуйтесь любимой поисковой программой, указав в качестве входной строки имя утилиты **Delpart.exe.**

Если последний способ не срабатывает, перепроверьте HCL-список для Windows 2003 на предмет возможных источников трудностей (более подробно о HCL-списке см. выше в разделе "Приобретайте только проверенное оборудование"). В противном случае попробуйте найти решение проблемы, обратившись к компакт-диску Microsoft TechNet или в группы новостей, посвященные Windows 2003, расположенные на Web-сервере news://msnews.microsoft.com.

Давайте рискнем (с VGA-режимом)

Вы обнаружите, что Windows 2003 совершенно не заботится о том, работает ли дисплей машины, на которой функционирует Windows Server 2003. Система Windows 2003 продолжает двигаться вперед, даже если вы не видите, что она делает, поскольку на экране отображается что-то совершенно беспорядочное или не отображается вообще ничего. Среди причин подобного поведения дисплея лидирует загрузка в дисплей драйвера, который не работает с вашим графическим адаптером, монитором или с тем и другим!

Если подобное произошло (а это распространенная проблема после установки), не паникуйте. Перезагрузите машину (нажмите кнопку перезагрузки на корпусе компьютера, если вы ничего не можете разобрать на экране). Чтобы получить доступ к дополнительным параметрам (Advanced Options), при появлении загрузочного меню нажмите клавишу <F8>, а затем щелкните на кнопке Enable VGA Mode (Включить режим VGA).

Подобные действия приводят к загрузке системы с использованием непритязательного VGA-драйвера. Затем вы можете попробовать различные драйверы (или перейти к поиску проблемы в оборудовании). В любом случае, прежде чем внести изменения в установки дисплея, нажмите кнопку проверки режима, чтобы убедиться, что дисплей работает в этом режиме.

Нет ничего лучше "хорошо известного старого"

После того как установка завершена, вы должны продолжить настройку конфигурации сервера Windows Server 2003, чтобы установить дополнительное ПО и добавить все типы информации, касающейся системы и политик пользователей, учетных записей и имен групп т.д.

Исходный загрузочный флоппи-диск сберегает систему!

Проблема с установочными дисками состоит в том, что утилита установки для загрузки Windows 2003 использует шесть из них. Использование этих дисков также вынуждает пройти длительную процедуру, прежде чем вы получите функционирующую машину. К счастью, творческие умы решили разработать исходный загрузочный флоппи-диск для Windows 2003. Он работает в любой системе и способен запустить любую самую неповоротливую машину под управлением Windows 2003. Вот как можно сформировать такой загрузочный флоппи-диск.

1. Отформатируйте дискету с помощью программы Windows Explorer (щелкните правой кнопкой мыши на пиктограмме с изображением дискеты в левой панели и выберите пункт меню Format (Форматировать)).
2. Отформатируйте эту дискету в системе Windows 2003, Дискеты, отформатированные в DOS, не будут работать как исходные загрузочные дискеты Windows 2003.
3. Проверьте установки утилиты Windows Explorer, чтобы убедиться, что вы можете видеть скрытые файлы. Для этого выберите команду Tools⇨Folder Options (Сервис⇨Свойства папки), выберите вкладку View (Вид), а затем щелкните на опции Show Hidden Files and Folders (Показывать скрытые файлы и папки) в разделе Advanced Settings (Дополнительные параметры).
4. Скопируйте следующие файлы из корневого каталога сервера на дискету, отформатированную в Windows 2003.
   - ✓ NTDLR
   - ✓ NTDETECT.COM
   - ✓ BOOT.INI
   - ✓ NTBOQTDD.SYS (только при его наличии)

В результате будет создана дискета, которая может привести в действие систему Windows 2003 без использования всех шести установочных дисков. Включите эти возможности в стандартный инструментарий для Windows 2003.

Если эта исходная загрузочная дискета не желает загружать систему, попробуйте использовать установочные дискеты к попытайтесь выполнить полное восстановление системы!

Всякий раз, когда вы вносите изменения в Windows 2003, они регистрируются в системном реестре, но иногда эти изменения имеют непредвиденные побочные эффекты (особенно если вы непосредственно редактируете реестр) и могут вызвать сбои в работе машины или даже проблемы с загрузкой.

Если ваша машина работает со сбоями или отказывается загружаться, всегда пробуйте вернуться к последней работающей версии реестра. При появлении загрузочного меню нажмите клавишу <F8>, чтобы получить доступ к меню Advanced Options, а затем выберите из него пункт Last Known Good Configuration. Эти действия означают откат к версии реестра, которая использовалась в последнее время вашей машиной для успешной загрузки. Положительный аспект такой процедуры состоит в том, что ваша машина, вероятно, будет загру-

жаться, отрицательный аспект связан с тем, что вы потеряете все изменения, которые внесли, начиная с последней перезагрузки машины.

После внесения большого количества изменений либо быстро создайте резервную копию реестра, либо быстро перезагрузитесь. Это позволит свести объем работы, который вы можете потерять (из-за непредсказуемых изменений реестра, неудачного выбора драйвера и т.п.), к минимуму.

Используйте для загрузки компакт-диск Windows 2003

Дистрибутивный компакт-диск Windows 2003 является загрузочным, поэтому вы можете загрузиться с него. Вам больше не нужно путаться в половине из дюжины загрузочных дискет для установки. Чтобы загрузить систему с компакт-диска, проверьте установки CMOS для загрузочного устройства.

Если ваша система не поддерживает загрузочный компакт-диск, то она устарела. Но если вы не в состоянии приобрести ничего нового, существует способ обойти ситуацию. Microsoft предлагает инструментарий компоновки загрузочной дискеты для установки, который вы можете загрузить с ее Web-узла. Перейдите в раздел Web-узла фирмы Microsoft, посвященный Windows 2003, по адресу www.microsoft.com/windowsserver2003/ и задайте в качестве ключа для поиска строку **setup disks for floppy boot install.**

Сомневаетесь? Выполните резервное копирование!

Windows 2003 — надежная операционная система, но она также подвержена случайностям, Поэтому позаботьтесь о том, чтобы создать резервную копию сервера Windows Server 2003, прежде чем вносить какие-либо существенные изменения в эту машину. К существенным изменениям относятся добавление пары новых пользователей или групп, внесение изменений в Active Directory, добавление служб или приложений, а также другие изменения, влияющие на содержимое реестра. Таким образом, если после внесения изменений произойдет отказ сервера, вы всегда сможете восстановить его после загрузки с установочных дисков и возврата сохраненного ПО к тому месту, с которого вы начали.

Подготовьтесь к реальной работе!

Хотя установка Windows Server 2003 — немалый подвиг, но реальная работа только начнется. Сформируйте, а затем претворяйте ваши планы в отношении домена и структур каталогов, имен машин, имен пользователей, имен групп и структур дисков из концепции в жизнь. Это реальная работа, которая превращает Windows Server 2003 в удобный инструмент для ваших пользователей, способный удовлетворить их запросы. Не забывайте регулярно резервировать систему!

Глава 23

Десять шагов к сетевой нирване с Windows Server 2003

В этой главе...

- Начнем с обычных подозрений
- Займемся маршрутизацией
- Устранение неполадок с IP-протоколом
- Ускорение работы сети
- Преодоление перегрузки сети
- Изучение сетевых служб
- Разрешение сетевых вопросов
- Отказ от изменений
- Учимся обращаться за помощью
- Лучше предупредить проблемы, чем исправлять их

Windows Server 2003 без сети подобна велосипеду без колес или чипсам без масла (заранее просим извинить любителей езды на одноколесном велосипеде и обезжиренной пищи).

Поскольку Windows Server 2003 и сети неразделимы, ваши пользователи могут быть очень недовольны, если сеть прекратит работу. Как бы вы ни старались избежать такой ситуации, время от времени она случается. Когда сеть "отдыхает, а вы по-прежнему находитесь в офисе, прочитайте нижеприведенные советы, чтобы ваше настроение улучшилось.

Никогда не упускайте очевидного

Причиной номер один отказа сети является (вы догадались) разрыв соединения. Всегда проверяйте плату сетевого интерфейса сервера, чтобы удостовериться в том, что кабели по-прежнему подключены или каким-то образом подсоединены. Также не забудьте проверить все концентраторы, маршрутизаторы, коробки ISDN (Integrated Services Digital Network — цифровая сеть с комплексными услугами), модем и все другие места, где проходят кабели (наподобие клиентской машины).

Специалисты по сетям часто говорят о "пирамиде выявления проблем", которая отражает усложнение сетевых возможностей начиная с оборудования и кабелей, через стек протоколов до приложения, которое запрашивает сетевые услуги. Очевидный смысл этой аналогии в том, что основание пирамиды значительно больше ее вершины. Эта пирамида иллюстрирует принцип, в соответствии с которым проблемы наиболее часто встречаются на физическом уровне сети. Почему? Потому что именно здесь находятся кабели и соединения. Идите и еще раз проверьте их.

Windows Server 2003 удачно позволяет вам подключить две или больше плат сетевого интерфейса или других устройств, которые могут переносить трафик, наподобие модемов, блоков ISDN или даже модулей обслуживания канала и данных (Channel Service Unit/Data Service Unit — CSU/DSU) для высокоскоростных цифровых сетей. Удвоение количества сетевых адаптеров (или других перечисленных устройств переноса трафика) позволяет Windows 2003 перемещать трафик с одного соединения на другое. Эта возможность, известная как *маршрутизация,* позволяет Windows Server 2003 соединять отдельные фрагменты сети.

Наиболее уязвимой и наиболее важной частью многих сетей оказывается звено, которое связывает локальную сеть с Internet (по крайней мере с вашим поставщиком услуг Internet). Если Windows 2003 выполняет эту роль в вашей сети, будьте готовы совершать регулярные ритуалы поиска неисправностей, чтобы сберечь это важное звено в работоспособном состоянии.

Если это возможно, изолируйте эту функцию, разместив ее на отдельном компьютере. Этот подход имеет два положительных аспекта.

- ✓ Добавление нагрузки на трафик маршрутизации и управление интерфейсом Internet требует дополнительного ПО и служб, которые могут обременить (возможно, перегрузить) Windows Server 2003.
- ✓ Вы должны ограничить влияние системных отказов как можно меньшим количеством служб. Вероятно, ваши пользователи будут менее неудовлетворенны, если потеряют только доступ к Internet или только доступ к сетевым файлам и приложениям, чем потеряв и то и другое одновременно.

Если вы используете Windows Server 2003 в качестве маршрутизатора, особенно, если в этом участвует Internet-канал, подумайте о том, чтобы установить на этой машине брандмауэр, например Proxy server от Microsoft или WinProxy от Ositis Software. Брандмауэр защитит вашу сеть от злоумышленников и позволит отслеживать и фильтровать входящую и исходящую информацию.

Инструментарий TCP/IP

Если вы намерены подключиться к Internet (а кто этого не делает в наши дни?), вам желательно сконструировать инструментарий TCP/IP, который поможет в разрешении ежедневных проблем, связанных с поддержанием сети TCP/IP в надлежащем состоянии.

К счастью, Windows 2003 включает отличный набор инструментов и утилит TCP/IP, которыми вы можете сразу воспользоваться. В табл. 23.1 перечислены некоторые первоочередные "кандидаты" на включение в ваш набор инструментов, предназначенный для выявления проблем протокола IP.

Таблица 23,1. Утилиты диагностики TCP/IP

Утилита	Описание
ARP	Отображает таблицу преобразования адресов, используемую IP-протоколом ARP (Address Resolution Protocol — протокол разрешения адресов). Помогает выявить неверные входы и обеспечивает соответствующее преобразование числовых IP-адресов в MAC-адреса (Media Access Control — протокол управления доступом к (передающей) среде)
HOSTNAME	Отображает IP-имя вашего хост-узла на экране. Используется для проверки текущего имени вашей машины
IPCONFIG	Отображает все текущие значения параметров сетевой конфигурации для всех интерфейсов. Используется для проверки назначения адресов для вашей машины, шлюза по умолчанию и маски подсети

Окончание табл. 23.1

Утилита	Описание
NBSTAT	Показывает статистику и активные соединения, использующие протокол NetBIOS поверх протокола TCP/IP. Используется для выявления проблем, связанных с правилами именования, предлагаемыми Microsoft
NETSTAT	Показывает активные соединения TCP и UDP (User Datagram Protocol — пользовательский протокол данных). Используется для проверки сетевых соединений и статистики протоколов TCP/IP
NSLOOKUP	Отображает информацию об известных DNS-серверах
PING	Проверяет базовые соединения с сетевыми компьютерами. Для проверки внутренних возможностей введите команду PING loopback, а затем проверьте локальные и удаленные машины, чтобы проверить общую возможность соединения
ROUTE	Отображает сетевые таблицы маршрутизации и позволяет вам их редактировать; полезна, прежде всего, при применении статической маршрутизации
TRACERT	Определяет маршрут от отправителя к получателю с помощью отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol — протокол управляющих сообщений в сети Internet), которые заставляют все станции между отправителем и получателем объявлять о себе

Установите быстрый сетевой адаптер на сервере

Для серверов Windows Server 2003 производительность имеет первостепенное значение. В сетевых средах, благодаря тому что трафик стремится перегрузить сервер, имеет смысл потратить дополнительные средства на быстрый, мощный сетевой адаптер. В качестве абсолютного минимума вам необходим PCI-совместимый адаптер, поскольку он обеспечивает наилучшее соединение шины с остальной частью системы. Ниже приведен перечень некоторых других усовершенствований сетевого адаптера для Windows Server 2003, которые стоит принять во внимание при его покупке.

- ✓ **Прямой доступ к памяти (Direct Memory Access — DMA).** Позволяет адаптеру передавать данные непосредственно из его встроенной памяти в память компьютера без запроса на участие в этом процессе ЦП.
- ✓ **Разделяемая память адаптера.** Позволяет отображать встроенную ОП адаптера в ОП компьютера. Когда компьютер "думает", что записывает данные в свою собственную ОП, он записывает их в память адаптера; а когда он "думает", что считывает данные из своей собственной памяти, он считывает их из памяти адаптера. Разделяемая системная память работает таким же образом, за исключением того, что адаптер считывает из памяти компьютера и записывает в нее, а не в свою собственную встроенную память. Дополнительная память для адаптера имеет почти такое же значение, как дополнительная память для ПК, работающего под управлением Windows 2003!
- ✓ **Управление шиной.** Позволяет адаптеру управлять шиной компьютера для координации передачи данных в память компьютера и из нее. Управление шиной позволяет ЦП концентрироваться на других видах деятельности и может повысить производительность от 20 до 70 процентов. Это наиболее стоящее усовершенствование из всех перечисленных выше.

- ✓ **Встроенный сопроцессор.** Добавляет дополнительный ЦП к сетевому адаптеру и позволяет ему обрабатывать данные, которые в противном случае должен обрабатывать ЦП компьютера. Сегодня многие сетевые адаптеры используют подобные процессоры для ускорения операций.

Основная идея всех перечисленных усовершенствований состоит в том, чтобы сосредоточить мощность и скорость обработки в том месте, где это наиболее целесообразно, — на сетевом адаптере, с которым должны взаимодействовать все пользователи, чтобы получать данные с сервера (или перемещать данные через сервер). Если у вас имеются средства, у вас может возникнуть желание исследовать магистральные сети зданий, которые используют запасные или высокоскоростные соединения, такие как FireWare (определяемое стандартом IEEE 1394), Fibre Channel, Asynchronous Transfer Mode (ATM) или Gigabit Ethernet.

Когда разделять, а когда властвовать

Когда трафик сетевого сегмента достигает высокого уровня, в сети случаются заторы, аналогичные пробкам на дорогах в часы пик. Когда такое случается, вам необходимо улучшить существующие дороги (перейти на более быструю сетевую технологию) или добавить новые дороги (разделить существующую сеть и поместить одну подсеть пользователей в одну часть, другую подсеть — в другую часть и т.д.).

Как вы можете определить момент, когда трафик начинает "душить" вашу сеть? Легко! Windows Server 2003 включает службу Network Monitor (Сетевой монитор) (нежно называемую NetMon), которую вы можете установить на сервере для наблюдения за его входящим и исходящим трафиком (а также проходящим через сегмент, к которому этот сервер подключен).

Служба NetMon не устанавливается на Windows Server 2003 по умолчанию, но ее легко добавить. Выберите команду Start⇨Control Panel⇨Add or Remove Programs⇨Add/Remove Windows Components⇨Management and Monitoring Tools (Пуск⇨Панель управления⇨Установка и удаление программ⇨Добавление и удаление компонентов Windows⇨Программы управления и мониторинга). Затем щелкните на кнопке Details (Подробности), установите флажок Network Monitor Tools (Средства сетевого мониторинга) и щелкните на кнопке OK. После выполнения описанных инструкций в папке Administrative Tools (Администрирование) появится пиктограмма NetMon.

Узнайте лучше утилиту NetMon, и вы намного лучше узнаете свою сеть!

Сомневаетесь? Проверьте службы!

Что делают сетевые серверы? Они обеспечивают сетевые услуги. Когда с сервером Windows Server 2003 что-то не так, но вы не видите ничего странного в поведении сети, обратитесь к утилите Services (Службы), окно которой показано на рис. 23.1.

Чтобы получить показанное отображение, выберите следующую последовательность команд меню: Start⇨Administrative Tools⇨Services (Пуск⇨Администрирование⇨Службы). Затем щелкните на пункте Services, чтобы отобразить список служб, установленных в текущий момент на сервере Windows Server 2003.

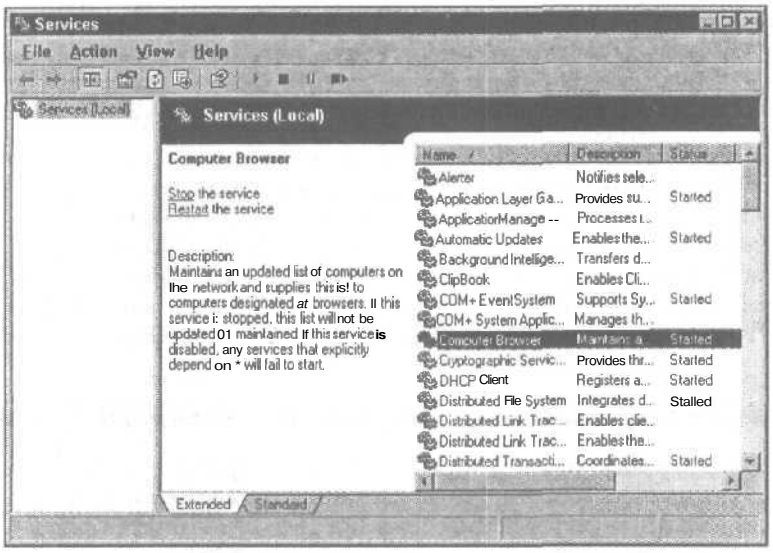


Рис. 23.1. Утилита Services указывает статус дня всех служб, установленных на сервере Windows Server 2003

Позаботьтесь о том, чтобы проверить пункты для основных служб, таких как Computer Browser, Services и Workstation. Убедитесь в том, что поле Status содержит значение Started и что значение поля Startup установлено правильно. (Для служб, запуск которых предусматривается при запуске системы, значение этого поля равно Automatic.)

Зачастую, когда в сети не появляется никаких очевидных проблем, вы можете обнаружить, что основная служба приостановлена, или остановлена, или отключена по какой-либо причине. Если служба остановлена, вы должны обратиться к утилите Event Viewer (Просмотр событий), чтобы выяснить причину, поскольку обычно остановленная служба указывает на серьезную проблему, которая может повториться.

Рационально работайте с именами и адресами

Единственный способ отыскать что-либо в сети — узнать адрес. Но, увы, люди значительно легче запоминают символические имена, чем числовые адреса (или, что еще хуже, магические двоичные образы, которыми пользуются компьютеры для взаимной адресации).

Это очень важно, когда вы имеете дело с работающей сетью, однако с точки зрения выявления проблем существуют два основных аспекта.

- ✓ Службы, которые осуществляют преобразование имен в адреса, должны быть правильно сконфигурированы и корректно работать, обеспечивая эффективное использование сети пользователями.
- ✓ Сетевые адреса, маски подсетей и соответствующая информация (наподобие шлюзов по умолчанию, адресов маршрутизаторов и т.д.) должны быть уникальны, корректно заданы и согласованы, чтобы компьютеры могли надлежащим образом использовать сеть.

Признаки проблем в этой области многочисленны и разнообразны. Дублирование адресов обычно приводит к тому, что все владельцы одного и того же адреса теряют способность доступа к сети. Неверные имена и адреса просто становятся недостижимыми и могут потребовать серьезных мер по устранению проблемы. Служба Active Directory может стать недоступной или неработоспособной по той или иной причине. (Вообще, тщательно проверяйте написание имен и числовые величины для адресов.)

К счастью, проблемы в этой области заявляют о себе в процессе настройки первоначальной конфигурации или при изменении установок. Если вы можете сравнить ваши установки и предположения с известным, рабочим набором значений, вы, как правило, сможете устранить эти проблемы быстро и безболезненно.

Следите за новшествами и отличиями

Следует иметь в виду, что источником многих сетевых проблем зачастую являются новшества и изменения, внесенные в сеть. Поэтому при исследовании сетевых неполадок сразу же задайтесь вопросами "Что нового?" и "Каковы отличия?", а затем как можно подробнее ответьте на них. В процессе разбора деталей вы зачастую можете вскрыть причины неполадок и найти способ их устранения одним стремительным маневром.

Опытные сетевые администраторы ведут журнал изменений и дополнений к их сетевым серверам, так что когда задаются подобные ключевые вопросы, ответы на них можно получить немедленно. Вы должны подражать этим профессионалам!

Если вам необходима помощь — обращайтесь

Иногда при поиске причины возникновения той или иной проблемы вы сталкиваетесь с мистикой или признаете, что не имеете ни малейшего представления о том, как ее решить. В подобных случаях не надо рвать на себе волосы — просто попросите помощи.

Иногда, для того чтобы иметь возможность решать проблемы Windows Server 2003, стоит заплатить 245 долларов за приобретение Technical Support Incident от Microsoft (цена интерактивного запроса — 99 долларов). Вы также можете обратиться к компакт-диску TechNet (его можно заказать на Web-узле `www.microsoft.com/technet`) или на Web-узел Microsoft Developer Network (www. `msdn.microsoft.com/`).

Если проблема связана с аппаратным обеспечением, проверьте, что можно получить на Web-узле изготовителя или с помощью доски объявлений для обновления драйверов. Если решение получить не удается, вам, возможно, также придется оплатить обращение за советом в службу технической поддержки изготовителя. Если вы можете определить основную причину проблемы, вы сможете получить помощь от тех, кто лучше знает ее. Даже если подобные расходы существенны для вас, подумайте о ценности времени (и своих нервах), которое вы сэкономите. Лучше зажечь свечу, чем проклинать темноту!

Проблемы лучше предупредить, чем исправлять

Лучший способ избавиться от сетевых и других типов системных проблем — это воспрепятствовать их появлению. Единственный способ избежать проблем и обеспечить нормальное функционирование сети — близко ознакомиться с сетевой средой и тщательно выяснить ее слабые стороны. Делать это следует до того, как сеть в полную силу проявит свои слабые стороны в виде отказа функционирования. Если вы следите за потенциально опасными областями и регулярно планируете операции резервирования, очистку файловой системы, пакетов обновления и исправляете текущие ошибки, вы сможете предупредить проблемы. И поверьте нам, предупреждение проблем означает не просто уменьшение объема работы, оно также приводит к значительному уменьшению распространения дурной славы, чем устранение ошибок после того, как они проявились. Не заставляйте себя обрести эту истину другим, тяжким путем!

Предметный указатель

Л

М

Н

О

П

P

C

T

У

Ф

Х

Ц

Ш

Э

Научно-популярное издание

Эд Титтел, Джеймс Майкл Стьюарт

Windows Sewer 2003 для "чайников"

В издании **использованы карикатуры американского художника** *Рича Теннанта*

Литературный редактор *И.А. Попова*

Верстка *А.В. Плаксюк*

Художественный редактор *В.Г. Павлютин*

Корректоры *З.В. Александрова, Л.А. Гордиенко, О.В. Мишутина, Л.В. Чернокозинская*

Издательский дом "Вильямс".
101509, Москва, ул. Лесная, д. 43, стр. 1.
Изд. лиц. ЛР № 090230 от 23.06.99
Госкомитета РФ по печати.

Подписано в печать 24.11.2003. Формат 70×100/16.
Гарнитура Times. Печать офсетная.
Усл. печ. л. 29,67. Уч.-изд. л. 25,30.
Тираж 4000 экз. Заказ № 1364.

Отпечатано с диапозитивов в ФГУП "Печатный двор"
Министерства РФ по делам печати,
телерадиовещания и средств массовых коммуникаций.
197110, Санкт-Петербург, Чкаловский пр., 15.

Важнейшие утилиты командной строки для TCP/IP

Каждая из этих утилит выполняет некоторые полезные функции. В столбце "Вызов справки" показано, как получить интерактивную помощь, касающуюся синтаксиса каждой команды.

Имя	*Файл запуска*	*Описание*
ARP	arp/h	Отображает и модифицирует таблицу преобразования адресов, поддерживаемую протоколом ARP
IPCONFIG	ipconfig/?	Отображает все текущие данные сетевой конфигурации TCP/IP
NETSTART	netstart/?	Отображает статистику протокола и текущие соединения TCP/IP
NSLOOKUP	nslookup	Отображает информацию о DNS-серверах
PING	ping	Проверяет соединения с локальными или удаленными компьютерами; отличное средство поиска неисправностей
ROUTE	route	Отображает сетевые таблицы маршрутизации и манипулирует ими
TRACERT	tracert	Отображает маршрут от вашей машины до заданного пункта назначения

Важнейшие сетевые команды

Каждая из этих команд выполняет некоторую полезную сетевую функцию NetBIOS. Чтобы получить справку общего характера, используйте команду Net help, а для получения справки по конкретной сетевой команде воспользуйтесь командой Net help <команда>.

Имя	***Описание***
Net accounts	Предназначена для управления учетными записями пользователей
Net computer	Добавляет или удаляет компьютеры из базы данных домена
Net help	Обеспечивает доступ ко всем справочным файлам сетевых команд
Net helpmsg	Объясняет сообщения об ошибках сетевых команд Windows
Net print	Позволяет просматривать задания на печать или управлять ими
Net send	Отправляет сообщения другим компьютерам или пользователям сети
Net share	Позволяет отображать, создавать и удалять сетевые ресурсы
Net use	Позволяет подключать и отключать компьютер от сетевого ресурса по имени

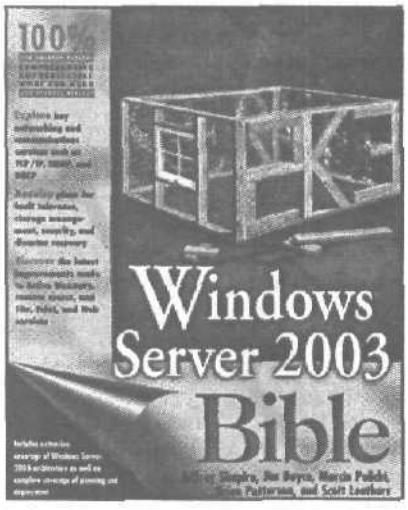
Средства администрирования Windows® Server 2003

Вы можете получить доступ к этим программам с помощью меню Start⇨Administrative Tools (Пуск⇨Администрирование) или ввода имени файла в диалоговом окне Run (Start⇨Run (Пуск⇨Выполнить))

Имя	Файл запуска	Описание
Active Directory Domains and Trusts (Домены Active Directory)	domain.msc	Управляет доверительными отношениями между доменами
Active Directory Sites and Services (Узлы и службы Active Directory)	dssite.msc	Управляет узлами, участвующими в тиражировании Active Directory
Active Directory Users and Computers (Пользователи и компьютеры Active Directory)	dsa.msc	Управляет пользователями, группами, компьютерами и другими объектами
Component Services (Службы компонентов)	comexp.msc	Управляет приложениями на основе COM+
Computer Management (Управление компьютером)	compmgmt.msc	Запускает и останавливает службы, управляет дисками и обеспечивает доступ к другим средствам управления компьютером для локального и удаленного администрирования
Data Sources (ODBC) (Источники данных)	odbcad.msc	Управляет ODBC-драйверами и источниками данных
DHCP	dhcpmgmt.msc	Управляет службой DHCP, которая присваивает параметры TCP/IP клиентам
Disk Defragmenter (Дефрагментация диска)	dfrg.msc	Запускает утилиту дефрагментации диска
Distributed File System (Распределенная файловая система)	dfscmd	Управляет службой DFS, которая создает единую сетевую иерархию из нескольких хост-узлов
DNS (Служба имен доменов)	dnsmgmt.msc/s	Управляет службой DNS, которая преобразовывает имена хостов в IP-адреса
Event Viewer (Просмотр событий)	eventvwr.msc/s	Обеспечивает доступ к различным файлам журналов Windows Server
Internet Service Manager (Управление службой Internet)	mmc.exe H:\W2KSVR\System 32\inetsrv\iis.msc	Управляет Web- и FTP-службами Internet
Licensing (Лицензирование)	llsmgr.exe	Управляет лицензиями и использованием клиентского ПО
Performance (Производительность)	perfmon.msc/s	Обеспечивает мониторинг производительности системы или сети
Routing and Remote Access (Маршрутизация и удаленный доступ)	rrasmgmt.msc/s	Управляет удаленными соединениями и маршрутизацией
Terminal Services Licensing (Лицензирование терминальных служб)	licmgr.exe	Управляет клиентским доступом к терминальным службам

WINDOWS SERVER 2003. БИБЛИЯ ПОЛЬЗОВАТЕЛЯ

Джеффри Шапиро,
Джим Бойс



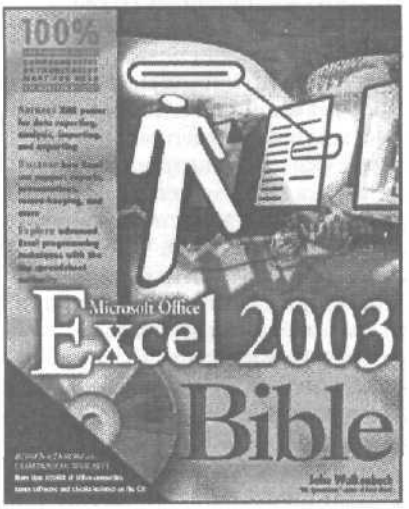
www.dialektika.com

Книга будет интересна всем, кто решил разобраться с новой версией сетевой операционной системы от Microsoft Windows 2003 Server. Авторы рассказывают о подготовительных действиях, установке и настройке параметров работы Windows 2003 Server. В книге подробно рассматривается служба каталогов Active Directory, а также различные сетевые и коммуникационные службы и протоколы. Уделяется внимание повышению безопасности системы, восстановлению системы после сбоев, а также всевозможным вопросам администрирования Windows 2003 Server, включая настройку службы печати, службы терминалов, Web-, FTP- и Intranet-служб. Для чтения книги не требуется специальной подготовки, но желательно иметь представление о семействе серверных операционных систем Windows, способах администрирования, утилитах обслуживания. Авторы дают практические советы, описывают рациональные приемы работы и рассказывают о стратегиях, которыми нужно руководствоваться при проектировании, развертывании и обслуживании сетей на базе Windows 2003 Server. Книга рассчитана на пользователей среднего и высокого уровня подготовки, а также на сетевых администраторов.

Плановая дата выхода
I кв. 2004 г.

EXCEL 2003. БИБЛИЯ ПОЛЬЗОВАТЕЛЯ

Джон Уокенбах



www.dialektika.com

Эта книга — полное руководство по самой мощной и в то же время простой в использовании программе электронных таблиц, Книга содержит все, что необходимо для изучения основ Excel и дальнейшей самостоятельной работы с этим программным продуктом. Здесь читатель найдет много полезных примеров, советов и приемов, которые в дальнейшем сможет применить на практике. Книга рассчитана на пользователей с различным уровнем подготовки. Легкий и доступный стиль изложения поможет даже новичкам быстро разобраться со всеми новыми возможностями Microsoft Office Excel 2003 и эффективно использовать их в своей повседневной работе.

Плановая дата выхода
II кв. 2004 г.

ПОИСК В INTERNET. САМОУЧИТЕЛЬ

Гусев В. С.

www.dialektika.com

Самоучитель предназначен для тех, кто уже получил элементарные навыки работы в Internet и понимает: в Сети имеется огромное количество чрезвычайно полезной информации, но найти ее не так просто. В книге даны подробные рекомендации по проведению поиска разнообразных данных с помощью наиболее популярных поисковых машин, порталов, каталогов и т.д. Приведены подробные инструкции по выполнению сложных запросов на поиск и многочисленные примеры, благодаря которым даже неискушенный пользователь сможет быстро находить в Internet необходимую ему информацию.

Плановая дата выхода
4 кв. 2003 г.

Мир интересных книг от издательской группы
"ДИАЛЕКТИКА - ВИЛЬЯМС"

ISBN 5-8459-0418-8

ISBN 5-8459-0461-7

ISBN 5-8459-0458-7

ISBN 5-8459-0358-0

ISBN 5-8459-0091-3

ISBN 5-8459-0079-4

ISBN 5-8459-0093-X

ISBN 5-8459-0092-1

ISBN 5-8459-0356-4

ISBN 5-8459-0005-0

ISBN 5-8459-0022-0

ISBN 5-8459-0434-X

... и много других книг Вы найдете на наших сайтах

www.dialektika.com

www.williamspublishing.com

Чтобы установить сеть и управлять ею — никакого опыта не требуется!

WILEY

ДИАЛЕКТИКА

Эта книга поможет вам:

- *освоить базовые концепции сетей*
- *понять основные принципы функционирования сетевого оборудования*
- *научиться устанавливать и обслуживать сетевую операционную систему*
- *узнать способы выявления неисправностей в сетях*

Откройте для себя Internet Information Services, Active Directory и многое другое

Благодаря этому руководству вы сможете легко установить, сконфигурировать, защитить сеть и управлять ею. Вы познакомитесь с основами компьютерных сетей, узнаете, как использовать новые "крутые" возможности Windows Server 2003, и быстро станете сетевым "гуру".

В стиле "ДЛЯ ЧАЙНИКОВ"

- *Объяснения простым и доступным языком*
- *Информация "без лишних подробностей"*
- *Пиктограммы и другие средства ориентирования в материале книги*
- *Шпаргалка, включающая самую ценную информацию*
- *"Великолепные десятки" советов*
- *Много юмора и шуток*

ISBN 5-8459-0559-1

Категория: операционные системы/Microsoft Windows Server 2003

Уровень: для начинающих и рядовых пользователей

Посетите "Диалектику" в Internet по адресу: http://www.dialektika.com

Об авторах

Эд Титтел — ветеран издательского дела, в активе которого несколько сотен журнальных статей и больше 100 книг. Эд работал над несколькими книгами из серии *...для "чайников"*, включая *HTML4 для "чайников"*, а также над книгами на другие темы. Эд руководит небольшой компанией LANWrights (Остин, штат Техас), которая специализируется на обучении, консультациях и публикациях в области компьютерных сетей.

Джеймс Майкл Стьюарт работает в сфере компьютерных технологий больше восемнадцати лет. Майкл — независимый консультант и инструктор, а также автор многих публикаций. Его работа в основном посвящена проблемам безопасности, Windows NT/2000/XP и Windows Server 2003, интрасетям и Internet. Майкл принимал участие в написании многочисленных книг, посвященных программам сертификации Microsoft; его статьи опубликованы в обычных и электронных изданиях.