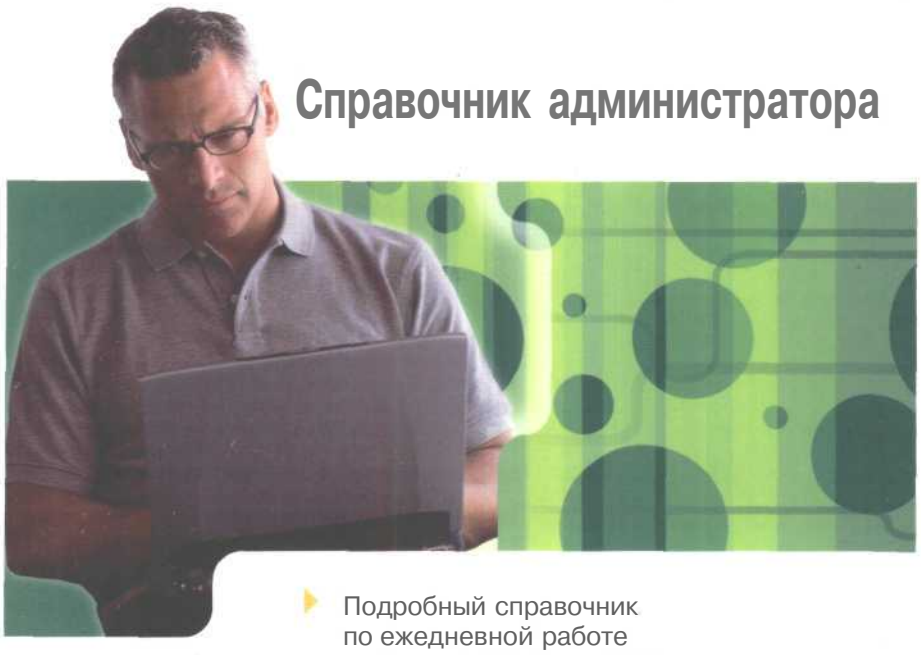
Уильям Р. Станек

Microsoft® Windows 2000

Справочник администратора



- Подробный справочник по ежедневной работе с Microsoft Windows 2000
- Таблицы, пошаговые инструкции, подробный предметный указатель

IT Professional

И РУССКАЯ РЕДАКЦИЯ

Microsoft®

William R. Stanek

Microsoft® Windows® 2000

Administrator's Pocket Consultant

Microsoft Press

Уильям **Р. Станек**

Microsoft® Windows® 2000

Справочник администратора

Москва 2002

РУССКАЯ РЕДАКЦИЯ

УДК 004.738.5
ББК 32.973.202
С76

Уильям Р. Станек
С76 Microsoft Windows 2000. Справочник администратора./Пер. с англ. — М.: Издательско-торговый дом «Русская **Редакция»,** 2002. - 592 с.: ил.

ISBN 5-7502-0193--7

Данная книга — краткий и исчерпывающий справочник для администраторов Microsoft Windows 2000 по всем основным вопросам, связанным с. выполнением типичных задач администрирования серверов и рабочих станций под управлением Windows 2000, включая управление службой каталогов Active Directory и другими ключевыми службами сервера **(DHCP,** WINS и DNS), учетными записями пользователей и групп, подключение и настройку жестких дисков, наборов томов, RAID-массивов, принтеров, а также устранение неполадок этих компонентов.

Книга адресована системным администраторам Windows 2000, опытным пользователям, выполняющим некоторые функции администраторов, а также администраторам, переходящим на Windows 2000 с Windows NT и других платформ.

Это богато иллюстрированное издание состоит из 19 глав и предметного указателя.

УДК 004.738.5
ББК 32.973.202

Подготовлено к изданию по лицензионному договору с Microsoft Corporation, Редмонд, Вашингтон. США.

ISBN 0-7356-0831-8 (англ)
ISBN 5-7502-0193-7

Оглавление

Благодарности

Работа над этой книгой доставила массу удовольствия, но имеете с тем потребовала предельного внимания. В ней описаны методики, которые я применяю ежедневно, и теперь не только я, но и все желающие смогут воспользоваться моими решениями. Но я не всесилен, а потому в работе над книгой мне помогало несколько человек, которых мне хотелось бы здесь упомянуть.

Как я уже писал в книгах *Microsoft Windows NT Server 4.0 Administrator's Pocket Consultant* и *Microsoft SQL Server 7.0 Administrator's Pocket Consultant,* команда Microsoft Press просто великолепна. Я очень благодарен Энн Хамильтон (Anne Hamilton) и Стюарту Стаплу (Stuart Stuple) за понимание моего практического потенциала и удачный подход к этой серии книг в целом. Джулиана Алдус (Juliana Aldous) помогла мне получить все необходимые инструменты. Джулия Миллер (Julie Miller), Марин Циммерман (Maureen Zimmerman) и Трэйси Томси (Tracy Thomsic) отлично руководили издательским процессом со стороны Microsoft Press, а Лайза Верл (Lisa Wehrle) — со стороны nSight, Inc. Я благодарен им за их профессионализм и скрупулезность.

К сожалению для автора (и к счастью для читателей), писательство — лишь одна сторона издательского процесса, вслед за которой идет серьезная редакторская работа. Должен сказать, что редактируют в Microsoft Press как нигде, а я успел поработать со многими издательствами. Техническими редакторами книги были Эбен Вербер (Eben Werbcr), Ричард Таха (Richard Taha) и Дэриан Таха (Darian Taha). Особое спасибо Ричарду, за комментарии к главам 14, 15 и 19 и помощь в самые напряженные моменты.

Также хочу поблагодарить литературное агентство Studio B и лично Дэвида Рогелберга (David Rogelberg) и Нила Салкинда (Neil Salkind).

Надеюсь, я никого не забыл, но если так, то не нарочно.

С уважением :-)

Введение

«Microsoft Windows 2000. Справочник администратора» задуман как краткий и исчерпывающий источник для администраторов Microsoft Windows 2000. Это печатное руководство по ресурсам, которое вы захотите всегда иметь под рукой. В книге затрагиваются все основные административные задачи по серверам и рабочим станциям на базе Windows 2000. Поскольку наша цель — максимум пользы в книге карманного размера, вам не придется искать среди сотен страниц посторонней информации то, что вам нужно. Теперь вы сразу найдете решение конкретной задачи.

Книга задумана как единый источник, к которому можно обращаться всякий раз, когда возникают вопросы по администрированию Windows 2000. Так что издание ориентировано на типичные процедуры администрирования, часто используемые задачи и документированные примеры. Одна из наших целей — сделать содержание сжатым, чтобы книга оставалась компактной и удобочитаемой, и в то же время максимально информативным. Теперь вместо талмуда в 1000 страниц или *100-страничной брошюрки* у вас есть ценное руководство по ресурсам, помогающее быстро и легко выполнять типичные задачи, решать проблемы и реализовывать такие продвинутые технологии Windows 2000, как Active Directory, DHCP, WINS и DNS.

Кому адресована эта книга

В нашей книге речь идет о версиях Windows 2000 для рабочей станции и сервера. Книга адресована

- системным администраторам Windows 2000,
- опытным пользователям, выполняющимнекоторые функции администраторов,
- администраторам, переходящим с Windows NT па Windows 2000,
- администраторам, переходящим на Windows 2000 с других платформ.

Чтобы сделать книгу максимально информативной, я исходил из того, что вы обладаете базовыми навыками сетевого администратора, в общих чертах знакомы с Windows 2000 и эта ОС уже установлена на ваших системах. Так что я не посвящаю целые главы описанию архитектуры, установке или запуску и завершению работы с Windows 2000. Но я описываю конфигурации Windows 2000 для рабочей станции и сервера, групповую политику, средства безопасности, аудит, резервирование данных, восстановление системы и многое другое.

Я также предполагаю, что вы хорошо знакомы с командами, процедурами и пользовательским интерфейсом Windows 2000. Если вам потребуется помощь для изучения основ Windows 2000, см. документацию по этой ОС.

Структура книги

Книга задумана для использования в повседневном администрировании сетей Windows 2000, а потому организована на основе прикладных задач, а не функций ОС, Читая эту книгу, вы должны знать о связи между сериями Pocket Consultants и Administrator's Companions. Обе книги задуманы как часть библиотеки администратора. Pocket Consultants — это книги сугубо практической направленности, Administrator's Companions — это полные пособия и справочники, затрагивающие любой аспект использования продукта или технологии на предприятии.

В книге есть подробное содержание и большой указатель для быстрого поиска решений. Также были добавлены многие другие средства ускорения поиска, включая пошаговые инструкции, списки, таблицы и массу перекрестных ссылок. Книга разбита на части и главы. Каждая часть содержит вводный параграф о главах внутри нес.

Часть I описывает основные задачи администрирования Windows 2000. В главе 1 дается обзор инструментов, методик и понятий администрирования Windows 2000. В главе 2 рассматриваются задачи управления системами на базе Windows 2000. Глава 3 посвящена процессам мониторинга, службам и событиям. В последней главе этой части речь об автоматизации административных задач, политик и процедур.

Во второй части описаны важные задачи администрирования учетных записей пользователей, компьютеров и групп.

Глава 5 знакомит со структурами службы Active Directory и поясняет, как работать с ее доменами. Б главе 6 рассматривается администрирование Active Directory; вы научитесь работать с учетными записями компьютера, контроллерами домена и организационными подразделениями. В главе 7 объясняется, как применять системные учетные записи, встроенные группы, права пользователей, встроенные возможности и скрытые группы, в сводных таблицах описано, когда использовать определенные типы учетных записей, прав и возможностей. Создание учетных записей пользователей и групп описано в главе 8. а управление ими — в главе 9.

Третья часть начинается с главы 10, где объясняется, как добавлять в систему жесткие диски и разбивать их на разделы, а также рассмотрены общие вопросы управления файловыми системами и дисками, включая дефрагментацию дисков, сжатие и шифрование файлов и т. п. Глава 11 посвящена управлению наборами томов и RAID-массивами, а также восстановлению поврежденных массивов, а глава 12 - управлению файлами и каталогами. Вы даже найдете советы по настройке внешнего вида папки по шаблонам. В главе 13 рассказано, как организовать общий доступ к файлам, томам и папкам для удаленных пользователей и из Интернета, а также обеспечить безопасность и провести аудит объектов Active Directory. В главе 14 рассматривается резервное копирование и восстановление данных, включая управление пулами носителей.

В заключительной части обсуждаются новейшие задачи администрирования. В главе 15 описаны важные моменты установки, настройки и тестирования протокола TCP/IP в системе Windows 2000 — от установки сетевых адаптеров до подключения компьютера к домену Windows 2000. Глава 16 начинается с руководства по устранению типичных неисправностей принтеров, затем рассматриваются вопросы установки и настройки локальных принтеров и сетевых серверов печати. Последние три главы в этом разделе посвящены ключевым службам Windows 2000: DHCP, WINS и DNS. DHCP используется для назначения динамических IP-адресов сетевым клиентам, WTNS - для разрешения имен компьютеров в IP-адреса, а DNS — для разрешения имен узлов R IP-адреса.

Условные обозначения

Я использовал множество элементов, чтобы текст был понятным и удобочитаемым. Коды и листинги набраны моноширинным шрифтом, кроме тех случаев, когда я явно говорю о вводе команды. В этом случае команда набирается **полужирным** начертанием. Когда я ввожу и определяю новый термин, я выделяю его *курсивом*.

Примечание описывает подробности акцентируемого момента.

Совет дает подсказку или дополнительную информацию.

Внимание! предупреждает о потенциальных проблемах.

Надеюсь, эта книга даст вам все необходимое для максимально быстрого и эффективного администрирования Windows 2000. Ваши комментарии автору присылайте по адресу *win2000-consulting@tvpress.com*. Спасибо.

Техническая поддержка

Издательский коллектив приложил все усилия, чтобы обеспечить точность информации в книге. Microsoft Press принимает поправки к книге по адресу *http://mspress.microsoft. com/support.*

Если у вас есть комментарии, вопросы или идеи, связанные с этой книгой, присылайте их в Microsoft Press одним из следующих способов.

Обычной почтой:

Microsoft Press
Attn: Microsoft Windows 2000
Administrator's Pocket Consultant Editor
One Microsoft Way
Redmond, WA 98052-6399

Электронной почтой:

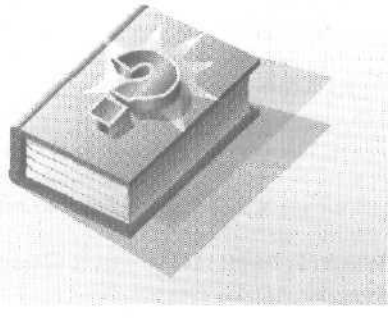
MSPINPUT@MICROSOFT.COM

Учтите, что поддержка продукта не предоставляется по указанным адресам. Сведения о поддержке продуктов Microsoft см. по адресу *http://www.microsoft.com/suppan.*

Часть I

Основы администрирования Windows 2000

Часть I посвящена основам администрирования Microsoft Windows 2000. В главе 1 дан обзор понятий, средств и методик администрирования Windows 2000. В главе 2 рассматриваются средства управления рабочими станциями и серверами Windows 2000. В главе 3 говорится о мониторинге событий и производительности. В главе 4 рассматривается автоматизация распространенных задач администрирования.



Глава 1

Обзор системного администрирования Windows 2000

Microsoft Windows 2000 — самая мощная ОС для ПК. Она предоставляет совершенно новый подход к средам рабочей станции и сервера и реализует новейшие концепции управления системой и администрирования. Вот некоторые из них.

- Active Directory — расширяемая и масштабируемая служба каталогов, использующая пространство имен, основанное па стандартной Интернет-службе именования доменов (Domain Name System, DNS).
- IntelliMirror — средства конфигурирования, поддерживающие зеркальное отображение пользовательских данных и параметры среды, а также центральное администрирование установки и обслуживания программного обеспечения.
- Terminal Services — службы терминалов, обеспечивающие удаленный вход в систему и управление другими системами Windows 2000.
- Windows Script Host — сервер сценариев Windows для автоматизации таких распространенных задач администрирования, как создание учетных записей пользователей и отчетов по журналам событий.

Хотя у Windows 2000 масса других возможностей, каждая из этих четырех оказывает большое влияние на выполнение задач администрирования. Наиболее эффективна технология Active Directory, фундаментально изменившая способы управления пользователями, группами и системами. Так что для успешной работы в качестве системного администратора Windows 2000 необходимо четко понимать структуры и процедуры Active Directory.

Microsoft Windows 2000 Professional и Server

Семейство ОС Windows 2000 состоит из версий Professional, Server, Advanced Server и Datacenter Server. У каждой свое назначение.

- **Windows 2000 Professional** разработана прежде всего для рабочих станций и сетевых клиентов. Она пришла на смену Windows 4.0 Workstation и обладает широким набором возможностей для конечных пользователей. Нацеленность на конечных пользователей выделяет Windows 2000 Professional среди серверных версий, поэтому данная редакция поддерживает ограниченный набор служб,
- **Windows** 2000 **Server** разработана для предоставления служб и ресурсов другим системам в сети. Она пришла на смену Windows NT 4.0 Server и обладает богатым набором функций и конфигурационных параметров. Windows 2000 Server поддерживает до двух центральных процессоров.
- **Windows 2000 Advanced Server** расширяет возможности Windows 2000 Server, обеспечивая балансировку загрузки, кластеризацию и поддержку конфигураций с большим объемом памяти (до 64 Гб) и четырьмя процессорами.
- **Windows 2000 Datacenter Server** — самый надежный Windows-сервер. Он поддерживает более сложную кластеризацию, чем Advanced Server и до 16 процессоров.

Примечание Разные редакции сервера поддерживают одинаковыз базовые функции и средства администрирования, т. е. методики, рассматриваемые в этой книге, можно применять независимо от того, какой редакцией Windows 2000 вы пользуетесь. Если у вас Windows 2000 Professional, установите средства администрирования Windows 2000 до выполнения задач администрирования.

При установке Windows 2000 система конфигурируется согласно ее роли в сети.

- Рабочие станции и серверы обычно становятся частью рабочей группы или домена.
- Рабочие группы — ото свободные объединения компьютеров, в которых каждый компьютер управляется независимо.

- Домены — это объединения компьютеров, коллективно управляемых контроллерами домена, т. е. серверами Windows 2000, регулирующими доступ к сети, базе данных каталога и общим ресурсам.

Контроллеры домена и рядовые серверы

При установке Windows 2000 Server в новую систему сервер можно конфигурировать как рядовой сервер, контроллер домена или изолированный сервер. Различие между этими типами серверов чрезвычайно важно. Рядовые серверы являются частью домена, но не хранят информацию каталога. Контроллеры домена отличаются от рядовых серверов, так как хранят данные каталога и выполняют службы аутентификации и каталога в рамках домена. Изолированные серверы не являются частью домена и имеют собственную БД пользователей, поэтому изолированный сервер также аутентифицирует запросы на вход.

Windows 2000 не различает основные и резервные контроллеры домена, так как поддерживает модель репликации с несколькими хозяевами. В этой модели любой контроллер домена может обрабатывать изменения каталога и затем автоматически реплицировать их на другие контроллеры домена. Это отличается от модели репликации с одним хозяином в Windows NT. где основной контроллер домена хранит главную копию каталога, а резервные — ее копии. Кроме того, Windows NT распространяла только БД диспетчера учетных записей безопасности (security access manager, SAM), а Windows 2000 — весь каталог информации, называемый *хранилищем данных.* В нем есть наборы объектов, представляющие учетные записи пользователей, групп и компьютеров, а также общие ресурсы, например серверы, файлы и принтеры.

Домены, использующие службы Active Directory, называют доменами Active Directory (или доменами Windows 2000), так как они отличаются от доменов Windows NT. Хотя Active Directory работает только с одним контроллером домена, в домене можно и нужно создать дополнительные контроллеры. Если один контроллер выходит из строя, для выполнения аутентификации и других важных задач можно задействовать другие.

В домене Active Directory любой рядовой сервер можно повысить до уровня контроллера домена, и без переустановки ОС, как того требовала Windows NT. Для повышения рядового сервера следует лишь установить на него компонент Active Directory. Также можно понизить уровень контроллера домена до уровня рядового сервера, если только сервер - не последний контроллер домена в сети. Для повышения и понижения уровня контроллеров домена служит мастер установки Active Directory;

1. Щелкните Start (Пуск).
2. Щелкните Run (Выполнить).
3. Наберите dcpromo в поле Open (Открыть) и щелкните OK.

Дополнительные компоненты и службы

В Windows 2000 большинство компонентов из пакета Option Pack для Windows NT сейчас интегрированы с ОС и включены в дистрибутивный CD-ROM как дополнительные компоненты. Например, добавив индексирующий компонент на сервер, вы сможете проиндексировать диски, папки и файлы для ускорения поиска. Если добавить службы транзакций, сервер сможет использовать Microsoft Distributed Transaction Coordinator для выполнения распределенных транзакций.

В Windows 2000 конфигурация сервера основана на службах, которые он предоставляет. Службы можно добавлять или удалять в любой момент, используя программу Configure Your Server (Настройка сервера):

1. Щелкните Start (Пуск).
2. Щелкните Programs (Программы).
3. Щелкните Administrative Tools (Администрирование) и выберите Configure Your Server (Настройка сервера).

Любой сервер может поддерживать одну или более следующих служб.

- Active Directory — сервер, предоставляющий службы каталога для домена (контроллер домена).
- File Server — сервер, предоставляющий файлы другим системам в сети.

- Print Server — сервер, управляющий принтерами и очередями печати.
- Web/Media Server — сервер, предоставляющий потоковые или Интернет-службы, или и то и другое, включая Web, File Transfer Protocol (FTP) и Simple Mail Transfer Protocol (SMTP).
- Networking Server — сервер, предоставляющий важные сетевые службы, включая Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), удаленный доступ или маршрутизацию.
- Application Server — сервер, обеспечивающий обмен сообщениями, работу баз данных и других типов бизнес-приложений клиент-сервер. Серверы приложений также могут обрабатывать групповую политику, обеспечивать функциональность IntelliMirror и служб терминалов.
- Advanced Server — сервер, сконфигурированный для использования таких нонеиших компонентов, как очередь сообщений, центр сертификации или удаленная установка.

Другие ресурсы Windows 2000

Перед изучением средств администрирования обратимся к другим ресурсам, которые можно использовать, чтобы упростить администрирование Windows 2000. Один из лучших ресурсов системного администратора — дистрибутивные диски Windows 2000. Они содержат всю необходимую информацию для внесения изменений в систему Windows 2000. Держите диски под рукой при изменении конфигурации системы. Скорее всего они вам понадобятся.

Чтобы не запускать дистрибутивный диск Windows 2000 всякий раз, при проведении системных изменений, можно скопировать каталог системного ресурса на сетевой диск. Например, на системе Intel можно скопировать каталог \i386 на сетевой диск. Когда вас попросят вставить компакт-диск и указать исходный каталог, просто укажите каталог на сетевом диске. Такая методика удобна и экономит время. Описание других полезных ресурсов см. ниже.

Средства поддержки Windows 2000

С дистрибутивного компакт-диска можно установить комплект ресурсов Windows 2000 - Resource Kit Support Tools. Средства поддержки — это универсальный набор утилит для

выполнения любых сервисных задач от диагностики системы до сетевого мониторинга.

Установка средств **поддержки** Средства поддержки устанавливаются так.

1. Вставьте установочный компакт-диск Windows 2000 в привод CD-ROM.
2. Когда появится окно автозапуска, щелкните Browse This CD (Обзор этого компакт-диска) — запустится Microsoft Windows Explorer (Проводник).
3. В Windows Explorer дважды щелкните Support, а затем — Tools.
4. Дважды щелкните Setup — запустится мастер установки средств поддержки Windows 2000. В диалоговом окно Welcome щелкните Next.
5. Введите пользовательскую информацию и щелкните Next.
6. Выберите тип установки: Typical или Custom. Если вы впервые используете средства поддержки, то можете установить все средства. Позже вы сможете удалить ненужные средства, перезапустив процесс установки и выбрав Add/Remove (Добавить/удалить).

Примечание В этой книге я говорю о двойном щелчке как наиболее распространенной методике, используемой для доступа к папкам и запуска программ. Первый щелчок выбирает элемент, второй — открывает (запускает) его. В Windows 2000 также можно настроить открытие/запуск одним щелчком. Здесь наведение указателя мыши на элемент выбирает его, а щелчок — открывает (запускает). Параметры щелчка позволяет изменять функция Folder Options (Свойства папки) из Control Panel (Панель управления). На вкладке General (Общие) выберите Single-Click To Open Item (Открывать одним щелчком, выделять указателем) или Double-Click To Open Item (Открывать двойным, а выделять одним щелчком).

7. Если вы выбрали стандартную или полную установку, дважды щелкните Next для запуска установки. При выборочной установке укажите добавляемые утилиты, а затем завершите установку.
8. Щелкните Finish. Выберите Yes для перезагрузки системы или No, если хотите перезагрузить систему позже.

Использование средств поддержки После установки доступ к средствам поддержки можно получать из консоли Windows 2000 Support Tools Console (рис, 1-1). Для запуска консоли щелкните Start Programs Windows 2000 Support Tools (Пуск\Программы\Windows 2000 Support Tools), а затем выберите Tools Management Console.

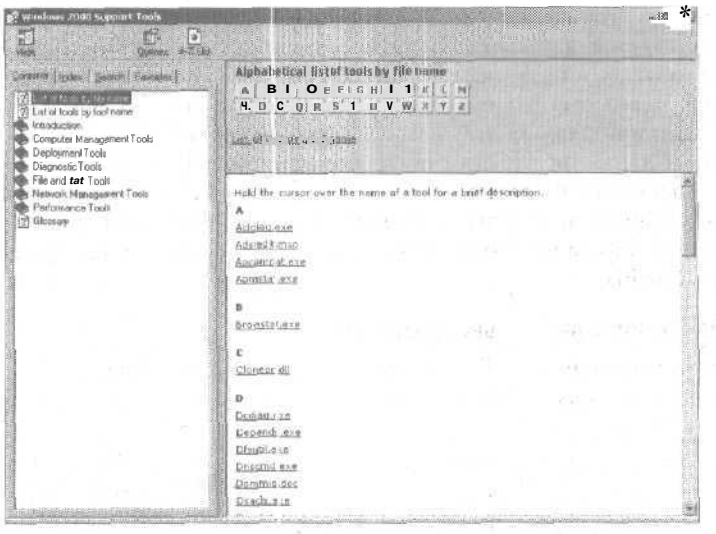


Рис. 1-1. Применяйте средства поддержки для выполнения таких задач, как диагностика системы и сетевой мониторинг.

Как видите, средства организованы по папкам, и к ним также можно получить доступ из списка. Дважды щелкнув List of Tools By File Name, вы увидите алфавитный список всех установленных средств поддержки.

Сервисные пакеты и заплатки

Как и в других ОС Windows, сервисные пакеты служат для распространения обновлений. При установке Windows 2000 также следует установить новейший сервисный пакет, если гарантирована его стабильная работа. Сервисные пакеты нумеруются последовательно, номер новейшего пакета – наивысший. Установив сервисный пакет, можно гарантировать стабильную работу рабочих станций и серверов,

Помимо сервисных пакетов существуют и заплатки (hot fix) для Windows 2000. Заплатки служит для устранения специ-

фичных проблем ОС. Поскольку большинство заплаток не подвергалось регрессивному тестированию, если у вас не возникает указанных проблем, не устанавливайте их.

Текущие сервисные пакеты и заплатки для Windows 2000 вы найдете на FTP-узле *(ftp://.microsoft.com/bussys/)* или на Web-узле Microsoft *(http://www.microsoft.com/support/)*. При доступе в этот каталог вы будете передвигаться по подкаталогам страны, языка и продукта. Большинство заплаток предлагаются в виде самоустанавливающихся исполняемых файлов. Перед установкой заплатки прочтите файл README.TXT в каталоге заплатки, В нем объясняется назначение заплатки, и даны инструкции по ее применению. Если вы хотите распаковать заплатку и изучить содержащиеся в ней файлы до установки, укажите имя исполняемого файла с параметром /x. Затем можно применять заплатку, используя программу HotFix.

Часто используемые средства

Есть много функций для администрирования рабочих станций и серверов Windows 2000. Чаще всего используются следующие.

- Панель управления — набор средств для конфигурации рабочей станции и сервера Windows 2000. К этим средствам можно обратиться, щелкнув Start (Пуск), выбрав Settings (Настройка), а затем — Control Panel (Панель управления).
- Графические средства администрирования — ключевые средства для управления компьютерами в сети и их ресурсами. Доступ к необходимому средству можно получить, щелкнув его значок в подменю Administrative Tools (Администрирование).
- **Мастера администрирования** — средства автоматизации ключевых административных задач. В отличие от Windows NT мастера не сосредоточены в центральном месте - доступ к ним происходит посредством выбора соответствующих параметров меню в других средствах администрирования.
- **Функции командной строки.** Большинство административных функций можно запускать из командной строки. Помимо этих утилит, Windows 2000 предоставляет и дру-

гие полезные в работе с системами на базе Windows 2000 инструменты.

В следующих разделах дано краткое введение в эти функции администрирования. В книге есть и дополнительные подробности для ключевых средстн. Помните: для применения этих программ вам может понадобиться учетная запись с привилегиями администратора.

Программы панели управления

Панель управления содержит программы для настройки системы (рис. 1-2).

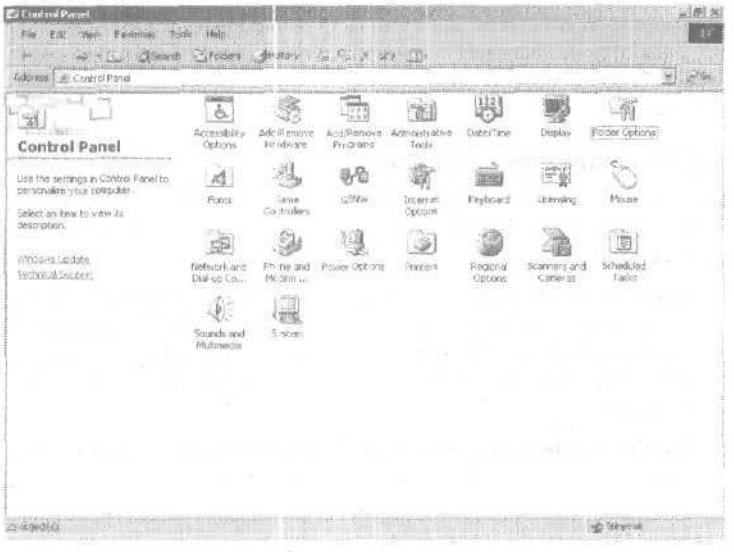


Рис. 1-2. Программы панели управления служат для настройки системы.

Основные программы, используемые при администрировании системы, перечислены ниже. Для запуска любой из них дважды щелкните ее значок и контрольной панели.

- Add/Remove Hardware (Установка оборудования) запускает Add/Remove Hardware Wizard (Мастер установки оборудования), позволяющий добавлять и удалять устройства и устранять аппаратные проблемы. Этот мастер

поможет также обновить конфигурацию устройств к их драйверы.

- **Add/Remove Programs** (Установка и удаление программ) служит для установки и автоматического удаления всех компонентов ПО, поддерживающего эту функцию. Также позволяет выбирать компоненты Windows 2000. Например, если при установке ОС вы не установили службы сертификации, их можно добавить позже.
- **Date/Time** (Дата и время) используется для просмотра или установки дня, времени и часового пояса. Вместо установки времени на отдельных компьютерах в домене вручную можно дать команду NET TIME для автоматической синхронизации времени. NET TIME можно применять в пользовательском сценарии входа для домена. В сценарии входа поместите команду NET TIME *имя_сервера* /set, где *имя_сервера* — сервер, с которым вы хотите синхронизировать время. О сценариях входа см. главу 6.
- **Display** (Экран) используется для конфигурации фонов, хранителей экрана, режима видеоизображения и параметров видео. Эту функцию также можно использовать для настройки вида значков па рабочем столе или визуальных эффектов, например постепенного свертывания меню. Для внесения изменений задайте параметры на вкладке Effects (Эффекты). Например, для отключения эффектов сбросьте флажок Use Transition Effects For Menus And Tooltips (Видеоэффекты для меню и подсказок).
- **Folder Options** (Свойства папки) регулирует многие параметры папок и файлов, включая тип рабочего стола, режимы просмотра папок, автономный режим использования файлов, а также количество щелчков для открытия файлов. Вы можете настроить на переносном компьютере автономные файлы, чтобы предоставить пользователям доступ к ключевым файлам, когда они не подключены к сети.
- Licensing (Лицензирование) служит для управления лицензиями на локальной системе с рабочей станции. На сервере она также позволяет изменять режим лицензирования установленных продуктов, таких как Windows 2000 Server или Microsoft SQL Server.

- **Network And Dial-Up Connections** (Сеть и удаленный доступ к сети) служит для просмотра сетевых реквизитов, добавления сетевых компонентов и установки сетевых соединений. Эту функцию также можно использовать для изменения имени компьютера и домена. Подробнее об этом см. главу 15.
- **Printers** (Принтеры) обеспечивает быстрый доступ к папке Printers, откуда можно управлять принтерами в системе. Об управлении сетевыми принтерами см. главу 16.
- **Scheduled Tasks** (Назначенные задания) позволяет просмотреть и добавить назначенные задания. Можно назначать выполнение задания однократно или периодически; подробнее об этом см. главу 4.
- **System** (Система) используется для отображения и управления свойствами системы, включая свойства запуска/остановки, переменные среды, профили оборудования и пользователей (см. также главу 2).

Графические средства администрирования

Windows 2000 предоставляет несколько типов средств системного администрирования. Чаще всего пользуются GUI-средствами. Обычно с помощью графических средств администрирования управляют той системой, на которой в настоящий момент работают, а также другими системами в доменах Windows 2000. Например, чтобы R консоли Component Services (Службы компонентов) выбрать компьютер, с которым вы хотите работать, щелкните правой кнопкой запись Event Viewer (Просмотр событий) в левой панели, затем выберите Connect To Another Computer (Подключиться к другому компьютеру): откроется диалоговое окно Select Computer (рис. 1-3). Щелкните Another Computer (Другим компьютером) и введите имя компьютера.

Основные графические средства администрирования

Ниже перечислены основные графические средства администрирования и их назначение (табл. 1-1). Для работы с ними щелкните их ярлык в подменю Administrative Tools (Администрирование).

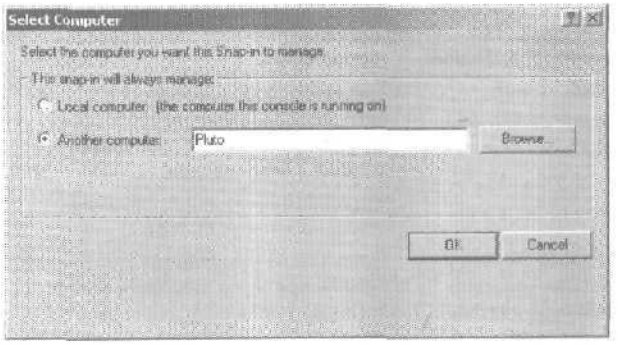


Рис. 1-3. Подключение к другому компьютеру позволяет управлять удаленными ресурсами.

Табл. 1-1. Краткий справочник основных средств администрирования Windows 2000.

Средство администрирования	Назначение
Active Directory Domains and Trusts (Active Directory — домены и доверие)	Управление доверительными отношениями между доменами
Active Directory Sites and . Services (Active Directory — сайты и службы)	Создание сайтов для управления репликацией Active Directory
Active Directory Users and Computers (Active Directory — пользователи и компьютеры)	Управление пользователями, группами, компьютерами и другими объектами в Active Directory
Component Services (Службы компонентов)	Конфигурация и управление приложениями COM+, управление событиями и службами
Computer Management (Управление компьютером)	Пуск и остановка служб, управление дисками и доступ к другим средствам управления системой
Configure Your Server (Настройка сервера)	Добавление, удаление и конфигурация служб Windows для сети
Data Sources (ODBC) [Источники данных (ODBC)]	Добавление, удаление и конфигурация источников данных и драйверов Open Database Connectivity (ODBC)
DHCP	Конфигурация и управление службой Dynamic Host Configuration Protocol (DHCP)

Табл. 1-1. *(продолжение)*

Средство администрирования	Назначение
Distributed File System (Распределенная файловая система DFS)	Создание и управление распределенными файловыми системами, объединяющими общие папки из разных компьютеров
DNS	Управление службой системы доменных имен (DNS)
Domain Controller Security Policy (Политика безопасности контроллера домена)	Создание и управление политикой безопасности на текущем контроллере домена
Domain Security Policy (Политика безопасности домена)	Создание и управление политикой безопасности на домене
Event Viewer (Просмотр событий)	Управление событиями и записями
Internet Authentication Service (Служба проверки подлинности в Интернете)	Управление аутентификацией, авторизацией и учетными записями удаленных пользователей Интернета
Internet Services Manager (Диспетчер служб Интернета)	Управление Web, FTP и SMTP серверами
Licensing (Лицензирование)	Управление лицензированием доступа клиентов к серверным продуктам
Local Security Policy (Локальная политика безопасности)	Управление политикой безопасности на локальном компьютере
Microsoft Network Monitor (Сетевой монитор)	Мониторинг сетевого трафика и устранение неисправностей в сети
Performance (Системный монитор)	Отображение графиков производительности системы и конфигурация журналов данных и сигналов оповещения
QoS Admission Control (Контроль допуска QoS)	Управление службой Quality of Service (QoS) Admissions Control для регулировки пропускной способности сети
Remote Storage (Внешнее хранилище)	Управление службой Remote Storage, автоматически переносящей редко используемые файлы с жесткого диска в **архивы** на ленте

Табл. 1-1. *(продолжение)*

Средство администрирования	Назначение
Routing and Remote Access (Маршрутизация и удаленный доступ к сети)	Конфигурация и управление службой Routing and Remote Access, контролирующей интерфейсы маршрутизации, динамическую IP-маршрутизацию и удаленный доступ
Server Extensions Administrator (Администратор серверных расширений)	Управление такими серверными расширениями, как FrontPage Server для Internet Information Server (IIS)
Telephony (Телефония)	Интегрирует IP-протокол в коммутируемую телефонную сеть общего пользования (Public Switched Telephone Network, PSTN)
Terminal Services Licensing (Лицензирование служб терминалов)	Управление лицензиями клиентского доступа к службам терминалов
WINS	Управление Windows Internet Name Service, преобразующей имена NetBIOS в IP-адреса и необходимой для обратной совместимости с Windows NT

Средства и конфигурация

Набор доступных средств администрирования на вашей системе зависит от се конфигурации. При добавлении служб на сервере устанавливаются средства управления этими службами. Они могут быть недоступны в Windows 2000 Professional. Тогда установите средства администрирования па вашей рабочей станции. Пакет Windows 2000 Administration Tools устанавливают так.

1. Зарегистрируйтесь на рабочей станции по учетной записи с привилегиями администратора.
2. Щелкните Start (Пуск), выберите Settings (Настройка) и щелкните Control Panel (Панель управления).
3. Дважды щелкните Add/Remove Programs (Установка и удаление программ).
4. Для добавления или изменения текущей конфигурации средств администрирования щелкните Change or Remove Programs (Замена или удаление программ), затем —Win-

dows 2000 Administration Tools. Раскроется элемент на правой панели. Щелкните Change (Изменить).

5. Для первой установки средств администрирования щелкните Add New Programs (Установка новой программы), а затем — CD or Floppy (CD или дискеты). Щелкните Next (Далее). В окне Run Installation Program (Запуск программы установки) выберите Browse (Обзор). В окне Browse (Обзор) дважды щелкните i386, выберите AdminPak.MSI и щелкните Finish (Готово).
6. Откроется окно мастера установки пакета администрирования Windows 2000. Щелкните Next. Выберите Install All Of The Administrative Tools, а затем — Next.
7. Средства администрирования будут установлены в вашу систему. Щелкните Finish (Готово) для завершения процесса.

Примечание Можно использовать ту же процедуру для добавления всех средств администрирования на сервер.

Функции командной строки

В Windows 2000 масса утилит командной строки. Многие из них используют протокол TCP/IP, поэтому следует предварительно установить TCP/IP.

Полезные функции

Как администратору, вам следует знать следующие утилиты командной строки:

- ARP отображает и управляет программно-аппаратной привязкой адресов, используемой Windows 2000 для отправки данных по локальной сети;
- AT назначает автозапуск программ по расписанию;
- FTP запускает встроенного FTP-клиента;
- HOSTNAME отображает имя компьютера в локальной системе;
- **IPCONFIG** отображает свойства TCP/IP для сетевых адаптеров, установленных в системе, также используется для обновления и освобождения выданных службой DHCP адресов;
- NBTSTAT отображает статистику и текущее соединение для протокола NetBIOS поверх TCP/IP;

- NET отображает семейство необходимых сетевых команд;
- NETSTAT отображает текущие TCP/IP соединения и статистику протокола;
- **NSLOOKUP** проверяет статус узла или IP-адреса при использовании с DNS.
- PING тестирует соединение с удаленным узлом;
- **ROUTE** управляет таблицами маршрутизации в системе;
- TRACERT во время тестирования определяет сетевой путь к удаленному узлу.

Чтобы научиться применять эти средства командной строки, наберите имя команды в командной строке без флагов: в большинстве случаев Windows 2000 выводит справку по использованию команды.

Использование NET-средств

Можно проще выполнять большинство задач, соответствующих NET-командам, используя графические средства администрирования и программы из Control Panel. Впрочем, некоторые NET-средства удобны для быстрого выполнения задач или для получения информации, особенно во время сеансов Telnet с удаленными системами:

- NET SEND отправляет сообщения пользователям, зарегистрированным в указанной системе;
- NET START запускает службу в системе;
- **NET STOP** останавливает службу в системе;
- NET TIME отображает текущее системное время или синхронизирует системное время с другим компьютером;
- NET USE подключает и отключает от общего ресурса.
- NET VIEW выводит список доступных сетевых ресурсов.

Чтобы научиться использовать NET-средства командной строки, наберите NET HELP и имя команды, например NET HELP SEND: Windows 2000 выведет справочные сведения.

Глава 2

Управление рабочими станциями и серверами Microsoft Windows 2000

Рабочие станции и серверы — основа сети Microsoft Windows 2000. Одна из основных функций администратора состоит в управлении этими ресурсами. Ключевой инструмент для этого — консоль Computer Management (Управление компьютером), предоставляющая единый интегрированный интерфейс для:

- получения общей информации о системном оборудовании, компонентах и программном обеспечении;
- управления сеансами и соединениями пользователя;
- управления пользованием файлами, каталогами и общими ресурсами;
- настройки административных оповещений;
- управления приложениями и сетевыми службами;
- конфигурации аппаратных устройств;
- просмотра и конфигурации дисков и съемных носителей информации.

Консоль Computer Management оптимальна для удаленного управления сетевыми ресурсами, но также нужно средство контроля над параметрами и свойствами системной среды. Здесь используется приложение System. Оно применяется для:

- конфигурации производительности приложения, виртуальной памяти и параметров реестра;
- управления системными и пользовательскими переменными среды;
- настройки стартовых и восстановительных системных параметров;
- управления аппаратными и пользовательскими профилями.

Управление сетевыми системами

Консоль Computer Management разработана для выполнения основных задач системного администрирования на локальных и удаленных системах. Вы часто будете работать с ней и должны детально ее знать. Запустить консоль Computer Management можно двумя способами:

- **выбрав** Start\Programs\Administrative Tools\Computer Management (Пуск\Программы\Администрирование\Управление компьютером);
- выбрав ComputerManagement (Управление компьютером) из папки Administrative Tools (Администрирование).

Главное окно разделено на две панели (рис. 2-1) и похоже на Windows Explorer (Проводник). Дерево консоли в левой панели служит для навигации и выбора средств, которые делятся на три категории;

- системные средства — средства общего назначения для управления системами и просмотра системной информации;

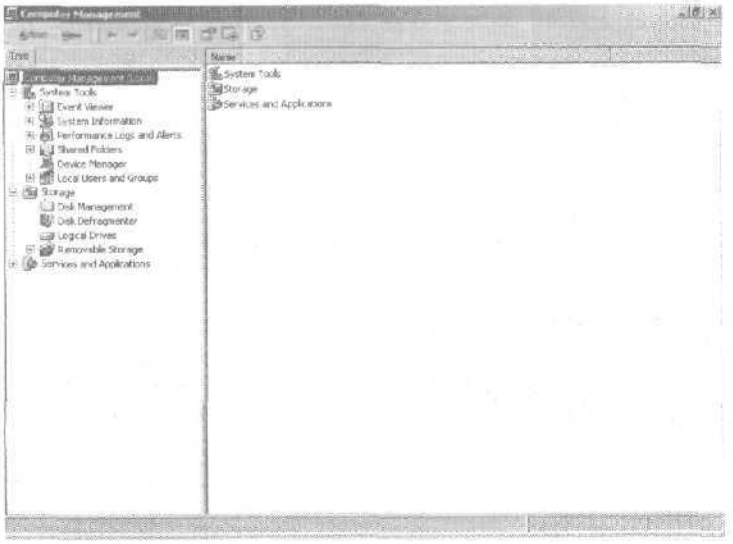


Рис. 2-1. Консоль Computer Management служит для управления компьютерами и ресурсами в сети.

- хранилище — здесь отображена информация о съемных и логических дисках и предоставляет доступ к средствам управления дисками;
- службы и приложения — обзор и управление свойствами служб и приложений, установленных на сервере.

Средства в дереве консоли определяют функциональность консоли Computer Management. Выбрав в дереве консоли Computer Management, вы получаете доступ к трем важным задачам:

- соединение с другими компьютерами;
- отправка консольных сообщений;
- экспорт информационных списков.

Соединение с другими компьютерами

Консоль Computer Management предназначена для работы с локальными и удаленными системами. Компьютер для управления можно выбрать, щелкнув правой кнопкой элемент Computer Management (Управление компьютером) в дереве консоли, а затем выбрав Connect to another Computer (Подключиться к другому компьютеру) в контекстном меню. Откроется диалоговое окно Select Object, где можно выбрать целевую систему.

1. В списке Look In (Искать в) выберите домен, с которым собираетесь работать (по умолчанию выбран текущий домен).
2. В списке объектов выберите компьютер или наберите имя компьютера в строке Name (Имя).

Отправка консольных сообщений

Консоль Computer Management позволяет отправлять сообщения пользователям удаленных систем. Эти сообщения появляются в диалоговом окне, которое пользователь должен щелкнуть, чтобы закрыть.

Сообщения удаленным пользователям отправляются в такой последовательности.

1. В консоли Computer Management щелкните правой кнопкой элемент Computer Management в дереве консоли. В контекстном меню выберите All Tasks (Все задачи), а за-

тем — Send Console Message (Отправка сообщения консоли). Откроется диалоговое окно (рис. 2-2).

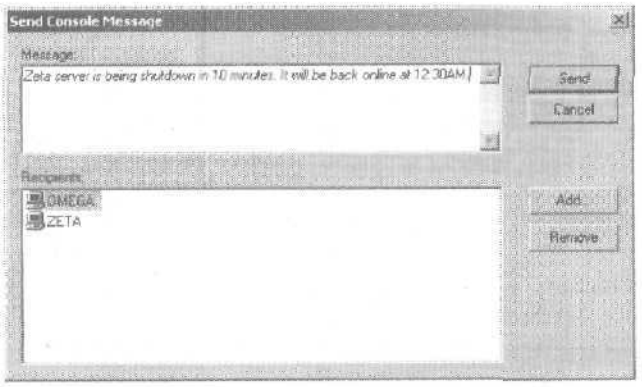


Рис. 2-2. Это диалоговое окно позволяет отправлять сообщения на другие системы.

2. Наберите текст сообщения в поле Message (Сообщение). В поле Recipients (Получатели) вы увидите имя компьютера, с которым вы связываетесь.
3. Чтобы отправить сообщение пользователям этой системы, щелкните Send. Кнопками Add (Добавить) и Remove (Удалить) можно добавить или удалить адресатов из списка. Приготовив сообщение к отправке, щелкните Send (Отправить).

Примечание Получать сообщения будут только пользователи, зарегистрированные на выбранной системе. Кроме того, системы Windows NT и Windows 2000 должны поддерживать службу Messenger для отправки и получения консольных сообщений. Системы с Windows 95/98, поддерживающие функцию WinPopup, также могут отправлять и получать сообщения.

Экспорт информационных списков

Возможность экспорта списков — одна из моих любимых функций консоли Computer Management, и если вы ведете записи системных сведений или регулярно работаете со сценариями Windows, она вам тоже пригодится. Функция Export List (Экспортировать список) позволяет сохранять инфор-

мацию, отображаемую на правой панели, в текстовом файле, разделяемом запятыми или табуляторами. Например, эта функция позволяет сохранять подробные сведения обо всех службах, работающих на системе.

1. В консоли Computer Management щелкните значок (+) рядом с узлом Services And Applications (Службы и приложения). Узел раскроется, и отобразятся его средства.
2. Щелкните правой кнопкой Services (Службы), затем из контекстного меню выберите Export List (Экспортировать список). Откроется диалоговое окно Save As (Сохранить как).
3. Выберите в списке Save In (Панка) место для сохранения, затем введите имя экспортируемого файла.
4. Выберите в списке Save As Type (Тип файла) формат экспортируемого файла. Колонки информации можно разделять табулятором или запятыми и сохранять текст в кодировке ASCII или Unicode. Чаще используется текст в кодировке ASCII.
5. Щелкните Save (Сохранить) для завершения экспорта.

Подобную процедуру можно выполнять и для экспорта списков с другой информацией из консоли Computer Management.

Подузел System Tools

Подузел System Tools (Служебные программы) в узле Computer Management служит для управления системами и просмотра сведений о системе. В подузле System Tools содержатся следующие служебные программы.

- Performance Logs And Alerts (Оповещения и журналы производительности) отслеживает производительность системы и создает журналы *на* основе параметров производительности. Это средство также применяется для уведомления или оповещения пользователей об условиях производительности. Подробнее о сигналах оповещения и мониторинге см. главу 3.
- Local Users And Groups (Локальные пользователи и группы) управляет локальными пользователями и локальными группами пользователей на выбранном компьютере. О работе с пользователями и группами см. часть II, там же говорится о других типах учетных записей, которые можно администрировать в службе Active Directory.

Примечание Локальные пользователи и локальные группы пользователей не являются частью Active Directory и управляются из консоли Local Users And Groups (Локальные пользователи и группы). У контроллеров домена нет записей в этой консоли.

- System Information (Сведения о системе) отображает сведения о системной конфигурации ресурсов оборудования и программной среды. Если вы хотите записать сведения о конфигурации в файл, используйте функцию Export List (Экспортировать список), описанную выше в разделе «Экспорт информационных списков».
- Services (Службы) управляет службами и свойствами служб. Как вы узнаете в главе 3, Windows 2000 обладает мощными функциями для эффективного управления службами.
- Shared Folders (Общие папки) управляет свойствами общих папок, сеансами пользователей и открытыми файлами (см. также главу 12).
- Event Viewer (Просмотр событий) — средство просмотра журналов событий на выбранном компьютере (см. также главу 3).
- Device Manager (Диспетчер устройств) — основное средство проверки состояния любого устройства, установленного на компьютере, и обновления драйверов. Его также можно использовать для устранения неполадок устройств. Об управлении устройствами см. ниже в этой главе.

Подузел Storage Tools

Подузел Storage Tools (Запоминающие устройства) узла Computer Management отображает сведения о дисках и предоставляет доступ к средствам управления дисками.

- Removable Storage (Съемные ЗУ) управляет портативными устройствами и ленточными библиотеками. Отслеживает рабочую очередь и запросы оператора, относящиеся к съемным носителям.
- Disk Defragmenter (Дефрагмснтация диска) решает проблемы дефрагментации, находя и комбинируя фрагментированные файлы.
- Logical Drives (Логические диски) отображает логические диски системы и управляет ими.

- Disk Management (Управление дисками) управляет жесткими дисками, разделами диска, наборами томов и дисковыми массивами. Заменяет программу Disk Administrator из Windows NT 4.0.

О работе с файлами, дисками и носителями информации см. часть III.

Работа со службами и приложениями

Любую задачу, относящуюся к приложению или службе, которую можно выполнить с помощью отдельного средства, можно выполнить и из узла Services And Applications (Службы и приложения). Например, если на выбранной системе установлен Dynamic Host Configuration Protocol (DHCP), то управлять DHCP можно через Services And Applications. Также можно выбрать средство DHCP из папки Administrative Tools (Администрирование). Подобные задачи можно выполнять любым из этих способов.

Это стало возможным, поскольку средство DHCP — оснастка Microsoft Management Console. Когда вы получаете доступ к средству DHCP в папке Administrative Tools, оснастка отображается в отдельной консоли. Когда вы получаете доступ к средству DHCP через узел Services And Applications, оснастка отображается в консоли Computer Management. О работе со службами и приложениями см. главу 3 и следующие.

Управление средой, профилями и свойствами системы

Приложение System (Система) служит для управления средой, профилями и свойствами системы. Запустите его, дважды щелкнув значок System (Система) в Control Panel (Панель управления). Откроется диалоговое окно, с пятью вкладками (рис. 2-3).

Вкладка General

Получить доступ к общим сведениям о системе на любой рабочей станции или сервере Windows 2000 можно через вкладку General (Общие) в приложении System (рис. 2-3).

На вкладке General перечислены:

- версия ОС;
- зарегистрированный владелец;
- серийный номер Windows 2000;
- тип компьютера;
- объем ОЗУ компьютера.

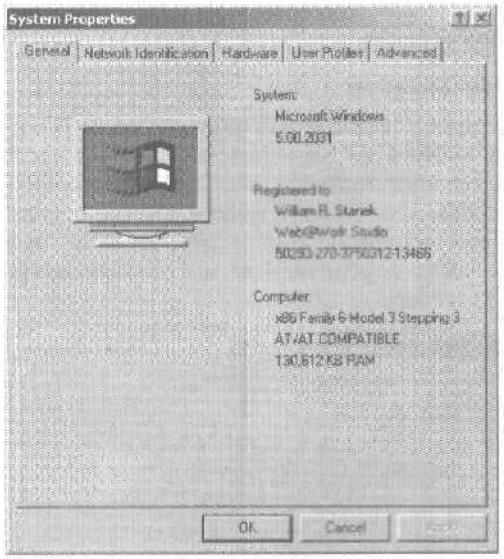


Рис. 2-3. Приложение System позволяет управлять переменными среды, профилями и свойствами системы.

Более подробный перечень сведений о системе вы получите в консоли Computer Management. Раскройте папку System Information (Сведения о системе) в подузле System Tools (Служебные программы), затем выберите System Summary (Сведения о системе). Информация в System Summary позволяет выяснить:

- название ОС, например Microsoft Windows 2000 Advanced Server;
- версию ОС, например 5.0.2381, где 5 — основная версия, О — номер редакции, а 2381 — номер сборки;
- изготовителя ОС;

- название и тип системы;
- процессор и версию системы базового ввода-вывода (BIOS);
- **установочный** каталог Windows;
- код страны и часовой пояс;
- общий объем доступной физической и виртуальной памяти;
- размер страничного файла.

Вкладка Network Identification

Сетевая идентификация компьютера отображается и модифицируется на вкладке Network Identification (Сетевая идентификация) в приложении System (рис. 2-4). На вкладке отображены полное доменное имя системы и данные о членстве в домене. Полное доменное имя — это, по сути, имя компьютера в DNS, также определяющее место компьютера в иерархии Active Directory.

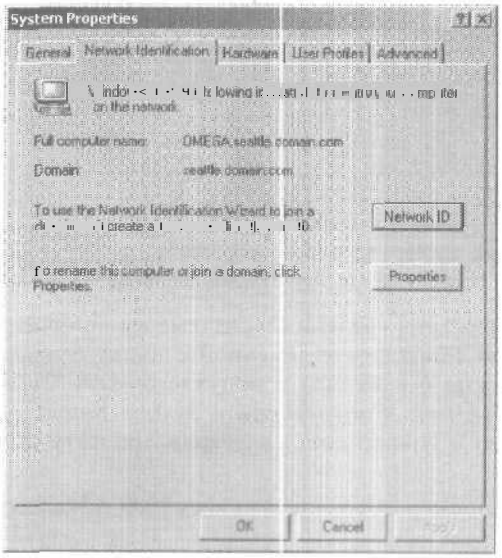


Рис. 2-4. Вкладка Network Identification позволяет настроить идентификацию системы, при этом идентификацию для контроллеров домена изменить нельзя.

Дважды щелкните значок System (Система) в Control Panel (Панель управления) и перейдите на вкладку Network Identification (Сетевая идентификация). Отсюда вы можете:

- щелкнув Network ID, запустить мастер сетевой идентификации, который поможет изменить информацию о сетевом доступе для компьютера;
- щелкнув Properties (Свойства), изменить имени системы и домена, с которым связан компьютер.

Примечание Нельзя изменять сетевые сведения о контроллере домена. Поэтому кнопки Network ID и Properties не нем недоступны. Изменить сетевые сведения о контроллере домена можно, понизив его до уровня рядового сервера, изменив нужные сведения, а затем снова повысив до уровня контроллера. Подробнее о повышении и понижении контроллера домена см. главу 6.

Вкладка Hardware

Рабочие станции и серверы Windows 2000 могут использовать разные профили оборудования. Профили оборудования необходимы переносным компьютерам, например ноутбукам: можно создать один профиль для его работы в сети (компьютер *пристыкован*), а другой — для автономного режима (компьютер *отстыкован*).

Конфигурация использования профилей оборудования

Для конфигурации профилей оборудования откройте вкладку Hardware (Оборудование) в приложении System, затем щелкните кнопку Hardware Profiles (Профили оборудования). Откроется диалоговое окно (рис. 2-5). Как и в системе с несколькими ОС. Windows 2000 позволяет настроить профили оборудования:

- выберите стандартный профиль, изменив позицию профиля в списке Available Hardware Profiles (Имеющиеся профили оборудования) — первым стоит профиль по умолчанию;
- укажите, сколько секунд система должна отображать стартовое меню профиля оборудования в поле Selecl The First Profile Listed If I Don't Select A Profile (Выбрать первый профиль в списке, если выбор не сделан за) — по умолчанию система ждет 30 секунд;

- выберите Wait Until I Select A Hardware Profile (Дождаться увного указания от пользователя), чтобы система ждала ответа пользователя.

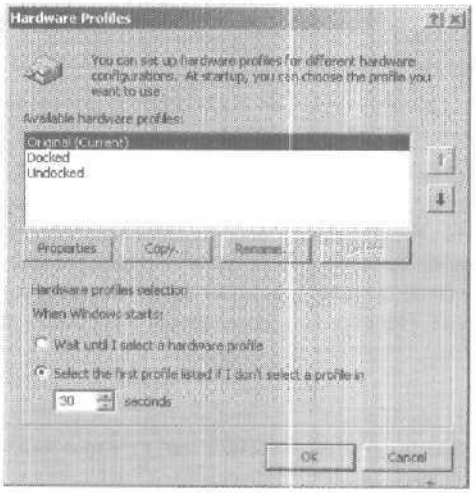


Рис. 2-5. Для любой системы на базе Windows 2000 можно настроить несколько профилей оборудования.

Настройка профилей для состояний **стыковки и расстыковки**

Эти профили конфигурируются так.

1. В списке Available Hardware Profiles (Имеющиеся профили оборудования) выберите исходный профиль и щелкните Copy (Копировать).
2. В диалоговом окне Copy Profile (Копирование профиля) наберите имя профиля — Docked — в поле To (В).
3. Выберите новый профиль и щелкните кнопку Properties (Свойства).
4. Пометьте флажок This Is A Portable Computer (Это портативный компьютер), а затем — переключатель The Computer Is Docked (Компьютер пристыковын).
5. Выберите Include This Profile As An Option When Windows Starts (Всегда выводить этот профиль как вариант при загрузке Windows). Щелкните OK.

6. Выберите исходный профиль в списке Available Hardware Profiles (Доступные профили оборудования), затем щелкните Copy (Копировать).
7. В диалоговом окне Copy Profile (Копирование профиля) наберите имя профиля — Undocked — в поле To (В).
S. Выберите новый профиль и щелкните кнопку Properties.
9. Пометьте флажок This Is A Portable Computer, затем The Computer Is Undocked (Компьютер отстыкован).
10. Выберите Include This Profile As An Option When Windows Starts, затем щелкните OK.
11. Укажите профиль оборудования для текущего состояния компьютера: стыкованного или отстыкованного.
12. Щелкните OK, чтобы завершить настройку.

Когда система будет загружена, пользователь сможет выбрать нужный профиль.

Вкладка User Profiles

Профили пользователя конфигурируются на вкладке User Profiles (Профили пользователей) приложения System (Система). Об управлении профилями пользователя в приложении System см. главу 9.

Вкладка Advanced

Производительность приложения и виртуальная память конфигурируются на вкладке Advanced (Дополнительно) приложения System (Система) (рис. 2-6).

Конфигурация производительности приложений

Производительность определяет время отклика активного приложения (в противовес фоновым приложениям, которые также могут выполняться на системе). Производительность приложений регулируется следующим образом.

1. Перейдите на Бкладку Advanced (Дополнительно) в приложении System, затем откройте диалоговое окно Performance Options (Параметры быстродействия), щелкнув одноименную кнопку
2. Для оптимизации времени отклика и оптимального доступа к ресурсам активного приложения *выберите* Applications (Приложений).

3. Чтобы ускорить время отклика фоновых приложений по сравнению с активным приложением, выберите Background Services (Служб, работающих в фоновом режиме).
4. Щелкните OK.

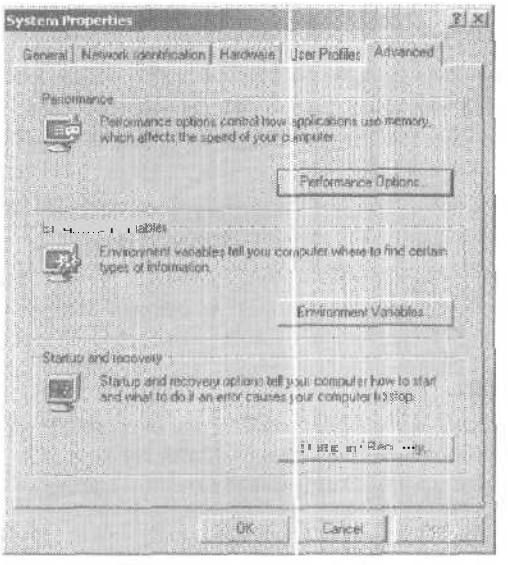


Рис. 2-6. Вкладка Advanced позволяет задать дополнительные параметры, включая параметры производительности, переменные среды, порядок запуска и восстановления.

Конфигурация виртуальной памяти

Виртуальная память позволяет задействовать дисковое пространство для расширения доступной оперативной памяти на системе. Эта функция используется, начиная с процессора Intel 386, — оперативная память записывается на диски путем *подкачки страниц.* При постраничной подкачке установленный объем оперативной памяти, например 32 Мб, записывается на диск как файл подкачки, и к нему при необходимости можно получить доступ на диске.

Первый файл полкачки создается автоматически для диска, содержащего ОС. Другие диски по умолчанию не содержат файлов подкачки, и их надо создавать вручную. При созда-

нии файла подкачки указывается начальный и максимальный размер. Файлы подкачки записываются на том под именем PAGEFILE.SYS.

Совет Microsoft рекомендует создавать файл подкачки для каждого физического тома в системе. На большинстве систем несколько файлов подкачки могут увеличить производительность виртуальной памяти. Вместо одного большого файла подкачки лучше иметь несколько небольших. Помните: съемным приводам не требуются файлы подкачки.

Конфигурация виртуальной памяти

Вот как сконфигурировать виртуальную память.

1. Запустите приложение System (Система) двойным щелчком значка System в Control Panel (Панель управления); затем выберите вкладку Advanced (Дополнительно).
2. Щелкните Performance Options (Параметры быстродействия), чтобы открыть диалоговое окно Performance Options. Затем выберите Change (Изменить), чтобы открыть окно Virtual Memory (Виртуальная память) (рис. 2-7).

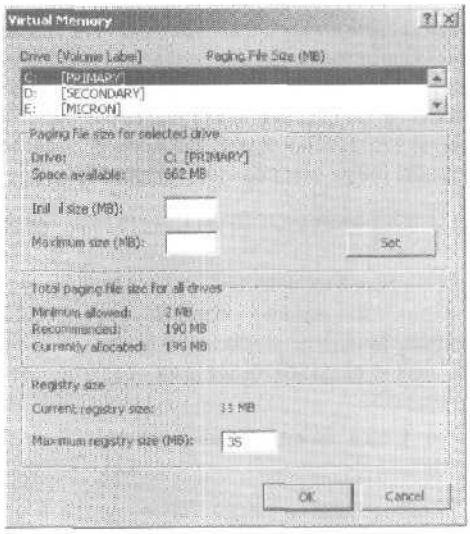


Рис. 2-7. Виртуальная память расширяет объем оперативной памяти на системе.

- Заголовок Drive (Диск) показывает, как виртуальная **память** сконфигурирована в системе **в данный** момент. **Каждому тому соответствует** свой **файл** подкачки. Диапазон значений файла подкачки **показывает** первоначальный **и максимальный размер.**
- Область Paging File Size For Selected Drive (Размер файла подкачки для выбранного диска) дает сведения о выбранном в данный момент диске и позволяет задать для него размер файла подкачки. Поле Space Available (Свободно) отражает размер свободного места на диске.
- Область Total Paging File Size For All Drives (Общий объем файла подкачки для всех дисков) дает рекомендуемый объем виртуальной оперативной памяти в системе и говорит, какой объем уже распределен. Если вы конфигурируете виртуальное ОЗУ впервые, то заметите, что рекомендуемый объем уже был задан для системного диска (в большинстве случаев).

Совет Хотя Windows 2000 может расширять файлы подкачки, наращивая их по мере надобности, в результате могут появляться фрагментированные файлы, что замедлит работу системы. Для оптимальной производительности задайте одинаковую величину для первоначального и максимального размера. В результате файл подкачки будет последовательным, и его можно будет записать в отдельный непрерывный файл (если это позволит объем тома).

3. В списке Drive (Диск) выберите том, с которым собираетесь работать.
4. В области Paging File Size For Selected Drive (Размер файла подкачки для выбранного диска) сконфигурируйте файл подкачки для диска. Введите первоначальный и максимальный размер, затем щелкните Set для сохранения изменений.
5. Повторите пп. 3 и 4 для каждого тома, который хотите сконфигурировать.

Примечание Файл подкачки также используется в целях отладки, когда в системе происходит ошибка STOP. Если файл подкачки на системном диске меньше минимального объема, требуемого для записи сведений по отладке в файл

подкачки, то эта функция будет отключена. Если вы хотите использовать отладку, минимальный размер файла должен быть равен объему оперативной памяти на системе. Например, система со 128 Мб ОЗУ требует файл подкачки размером 128 Мб на системном диске.

6. Щелкните OK и, если потребуется, замените существующий PAGEFILE.SYS, щелкнув Yes (Да).
7. Закройте приложение System и выберите Yes, чтобы перезагрузить систему.

Настройка **размера реестра**

Windows 2000 позволяет контролировать максимальный объем памяти и дискового пространства, используемого реестром. Ограничение размера реестра заранее не выделяет под него место на диске и не гарантирует доступность места при необходимости расширения. Пространство используется только по мере необходимости до максимально разрешенного значения.

1. Войдите в систему под учетной записью с привилегиями администратора.
2. Запустите приложение System (Система), дважды щелкнув значок System в Control Panel (Панель управления), и перейдите на вкладку Advanced (Дополнительно).
3. Выберите Performance Options (Параметры быстродействия), чтобы открыть окно Performance Options. Затем щелкните Change (Изменить), чтобы открыть окно Virtual Memory (Виртуальная память).
4. В диалоговом окне Virtual Memory (Виртуальная память) введите новый максимальный размер реестра в поле Maximum Registry Size (Максимальный размер).

Конфигурация переменных среды для системы и пользователя

Переменные среды системы и пользователя конфигурируются в диалоговом окне Environment Variables (рис. 2-8). Чтобы открыть это окно, запустите приложение System, дважды щелкнув значок System в Control Panel, затем на вкладке Advanced (Дополнительно) щелкните кнопку Environment Variables (Переменные среды).

Рис. 2-8. Диалоговое окно Environment Variables позволяет конфигурировать переменные среды для системы и пользователя.

Создание переменной среды

Переменные среды можно создавать следующим образом.

1. Щелкните кнопку New (Создать) под списком System Variables (Системные переменные) или User Variables (Переменные среды пользователя) в зависимости от того, какого типа переменную хотите создать. Откроется окно New System Variable (Новая системная переменная) или New User Variable (Новая пользовательская переменная).
2. В поле Variable Name (Имя переменной) наберите имя переменной. Затем в поле Variable Value (Значение переменной) наберите значение переменной.
3. Щелкните OK.

Редактирование переменной среды

Существующую переменную среды можно изменить.

1. Выберите переменную в списке System Variables или User Variables.
2. Щелкните кнопку Edit (Изменить) под списком System Variables или User Variables, в зависимости от типа мо-

дифицируемой переменной откроется диалоговое окно Edit System Variable (Изменение системной переменной) или Edit User Variable (Изменение пользовательской переменной).

3. Введите новое значение **в поле** Variable Value (Значение переменной).
4. Щелкните OK.

Удаление переменной среды

Переменную среды можно удалить, выбрав в списке и щелкнув кнопку Delete (Удалить).

Примечание При создании или редактировании переменных среды для системы изменения вступают в силу только после перезагрузки. При создании или корректировке переменных среды изменения для пользователя вступают в силу, когда он в следующий раз входит в систему.

Настройка запуска и восстановления системы

Свойства запуска и восстановления системы конфигурируются в диалоговом окне Startup And Recovery (рис. 2-9). Чтобы открыть его, запустите приложение System, дважды щелкнув значок System в Control Panel. Затем на вкладке Advanced щелкните кнопку Startup And Recovery (Загрузка и восстановление).

Настройка параметров запуска

Область System Startup (Загрузка операционной системы) в окне Startup And Recovery управляет запуском системы. Выберите ОС по умолчанию из списка Default Operating System (Операционная система по умолчанию). Эти параметры берутся из раздела ОС в системном файле BOOT.INI.

При загрузке Windows 2000 по умолчанию отображает меню запуска ОС в течение 30 секунд. Вы можете:

- сразу загрузить ОС по умолчанию, сбросив флажок Display List Of Operating Systems For (Отображать список операционныхсистем);
- отобразить доступные параметры на *некоторое* время, пометив флажок Display List Of Operating Systems For и задав задержку в секундах.

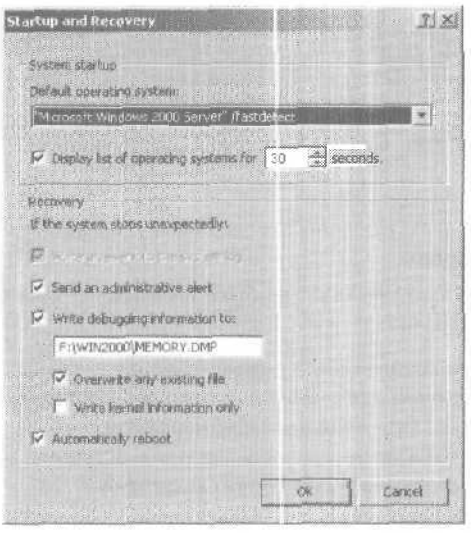


Рис. 2-9. Процедура запуска и восстановления системы конфигурируется в диалоговом окне Startup And Recovery.

Обычно на большинстве систем для выбора достаточно 3-5 секунд: это не замедлит процесс загрузки системы.

Настройка параметров восстановления

Параметры восстановления позволяют администраторам контролировать происходящее при возникновении в системе неисправимой ошибки (также известной как ошибка STOP). Эти параметры можно установить на вкладке Startup/Shutdown:

- Write an event to the system log (Записать событие в системный журнал) — регистрация ошибки в журнале системы, что позволяет администраторам позже просмотреть ошибку, используя консоль Event Viewer (Просмотр событий);
- Send an administrative alert (Отправить административное оповещение) отправляет сообщение адресатам, указанным в диалоговом окне Alert;
- **Write** debugging information (Запись отладочной информации) — при выборе режима дампа система записывает отладочную информацию в файл, по которому можно

диагностировать проблему (при включении этого параметра следует указать имя файла);

- **Overwrite** any existing **file** (Затирать существующий файл) гарантирует, что любые существующие файлы дампа будут заменены, если произойдет новая ошибка STOP, что актуально, если у вас мало свободного места на диске;

Совет Полный дамп памяти можно создать, только если система правильно сконфигурирована. Системный диск должен иметь файл подкачки памяти достаточно большого размера (устанавливается, как и виртуальная память, на вкладке Advanced), а диск, на котором записан файл дампа, должен иметь столько же свободного места. Так, на моем сервере 128 Мб оперативной памяти, и он требует файл подкачки на системном диске такого же размера - минимум 128 Мб. Поскольку тот же диск используется под файл дампа, на диске должно быть минимум 256 Мб свободного места для корректного сохранения отладочных сведений (т, е. 128 Мб для файла подкачки и еще 128 Мб для дампа).

- Automatically reboot (Выполнить автоматическую перезагрузку) — пометьте этот флажок, чтобы система перезагружалась, если произойдет ошибка.

Примечание Автоматическая перезагрузка не всегда хороша. Иногда нужно просто остановить работу ОС, чтобы вы обратили внимание на ошибку, а не сразу перезагрузить систему. Иначе вы узнаете, что ОС перезагружалась, лишь когда просмотрите системный журнал или увидите монитор системы в момент перезагрузки.

Управление аппаратными устройствами и драйверами

В Windows 2000 три основных инструмента для управления аппаратными устройствами и драйверами:

- Device Manager (Диспетчер устройств);
- Add/Remove Hardware Wizard (Мастер установки и удаления оборудования);
- Hardware Troubleshooter (Средство устранения неполадок).

Эти средства используются при установке, удалении или устранении неисправностей аппаратных устройств и драйверов.

Обзор и управление аппаратными устройствами

Вы можете просмотреть подробный список всех аппаратных устройств, установленных па системе.

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Computer Management (Управление компьютером).
2. В консоли Computer Management щелкните значок (+) рядом с узлом System Tools (Служебные программы).
3. Выберите Device Manager (Диспетчер устройств). Появится полный список системных устройств, по умолчанию упорядоченный по их типу,
4. Щелкните значок (+) рядом с типом устройства, чтобы открыть список конкретных экземпляров данного типа устройств.
5. Щелкнув правой кнопкой запись устройства, вы сможете управлять устройством командами контекстного меню. Доступные параметры зависят от типа устройства, но всегда включают следующие:
   - Properties (Свойства) отображает диалоговое окно свойств устройства;
   - Uninstall (Удаление) удаляет устройство и его драйвер;
   - Disable (Отключить) отключает устройство, но не удаляет его;
   - Enable (Включить) включает устройство, если оно отключено.

Совет В списке устройств отображаются предупреждающие символы, если устройство работает с ошибками. Желтый символ с восклицательным знаком указывает, что с устройством проблема. Красный X указывает, что устройство было неправильно установлено или почему-либо отключено пользователем или администратором.

Команды в меню View (Вид) консоли Computer Management служат, чтобы изменить стандартные параметры отображения типов устройств и способа их перечисления.

- Devices by type (Устройства по типу) —отображение по типу установленного устройства, например группировка жестких дисков или принтеров (вил по умолчанию).

- **Devices by** connection (Устройства по подключению) - отображение по типу подключения, например, в этом виде отображается системная плата и диспетчер логических дисков.
- **Resources by type** (Ресурсы по тину) — отображение состояния выделенных ресурсов по типу устройства, их использующего. Под тинами ресурсов подразумеваются DMA-каналы, порты ввода-вывода, запрос прерывания (IRQ) и адреса памяти.
- **Resources by connection** (Ресурсы по подключению) - отображение состояния всех выделенных ресурсов по типу подключения, а не по типу устройства.
- **Show hidden** devices (Показать скрытые устройства) - отображение устройств, не поддерживающих Plug and Play, а также устройств, отключенных от компьютера, но драйверы которых не были удалены.

Установка и удаление драйверов устройств

Для поддержки устойчивой работы устройств важно иметь текущие версии драйверов. Вот как их установить.

1. В консоли Computer Management (Управление компьютером) откройте Device Manager (Диспетчер устройств).
2. Устройства можно перечислить по типу, ресурсу или подключению. Щелкните правой кнопкой подключение, которым хотите управлять, и выберите команду Properties (Свойства). Откроется диалоговое окно свойств данного устройства.
3. Для удаления драйвера устройства (и соответствующего устройства) на вкладке Driver (Драйвер) щелкните кнопку Uninstall (Удалить). Чтобы подтвердить удаление, щелкните OK.
4. Чтобы установить или переустановить драйверы, на вкладке Driver щелкните Update Driver (Обновить драйвер) для запуска мастера обновления драйверов. В первом окне мастера щелкните Next (Далее).

Совет Обновленные драйверы могут добавить функциональность устройству, улучшить производительность и решить проблемы. Однако не следует устанавливать последнюю версию драйвера на рабочий сервер без тестирования в лабораторной среде.

5. **Вы можете решать:** искать драйверы **или выбрать из** списка **известных** драйверов (рис. 2-10).

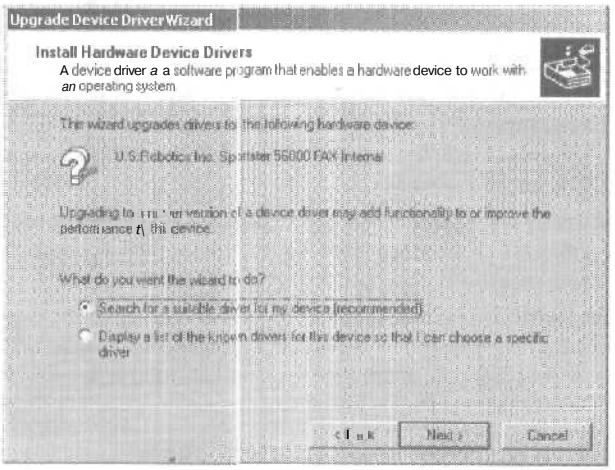


Рис. 2-10. Решите, искать ли нужные драйверы или выбрать из списка известных драйверов.

6. В последнем случае нужно указать тип устройства, например Modem (Модем) или Network Adapter (Сетевая плата). Затем мастер отобразит окно выбора (рис. 2-11). Найдите в списке слева изготовителя, а затем в списке справа — ваше устройство.

Если вы ищете драйверы, мастер просматривает системную БД драйверов, а также любые дополнительные места размещения драйверов, которые вы укажете, например, дисковод или привод CD-ROM. Отображаются любые совпадающие драйверы, и вы можете выбрать подходящий.

Примечание Если изготовителя или устройства, которое вы собираетесь использовать, нет в списке, вставьте диск с драйвером для устройства в дисковод и щелкните кнопку Have Disk (Установить с диска). Следуйте инструкциям и выберите нужное устройство.

После выбора драйвера устройства продолжайте процесс установки, щелкнув Next. Щелкните Finish (Готово), когда установка драйвера будет завершена.

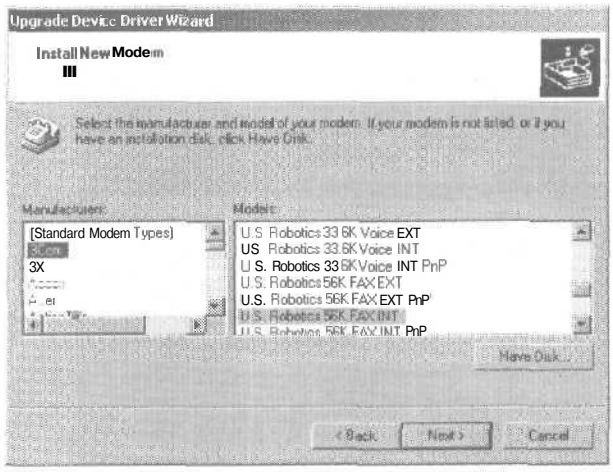


Рис. 2-11. Выберите драйвер устройства по изготовителю и модели.

Установка, удаление и устранение неполадок оборудования

Аппаратные устройства можно устанавливать и удалять, используя мастер. Он же поможет устранить неполадки существующего оборудования.

1. Запустите приложение System, дважды щелкнув значок System в Control Panel. На вкладке Hardware (*Оборудование*) щелкните кнопку Hardware Wizard (Мастер оборудования).
2. Для установки нового оборудования или устранения неполадок в существующем выберите Add/Troubleshoot A Device (Добавить/провести диагностику устройства) (рис. 2-12).
3. Для удаления оборудования выберите Uninstall/Unplug A Device (Удалить/извлечь устройство).
4. О процедурах установки, удаления и устранения неисправностей см. ниже.

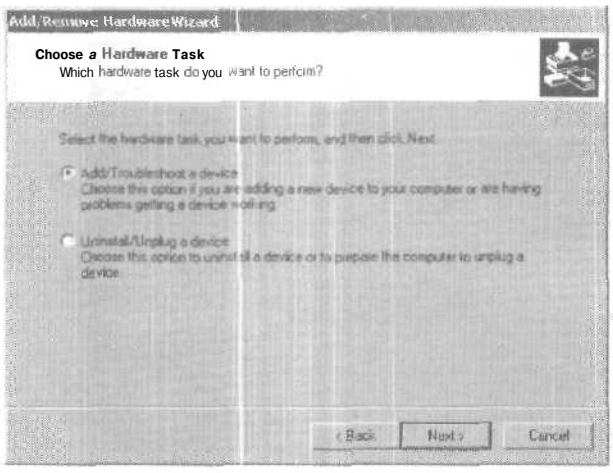


Рис. 2-12. Мастер поможет установить, удалить или устранить неисправности аппаратных устройств.

Установка оборудования

Технология Plug and Play, реализованная в Windows 2000, хорошо справляется с задачей обнаружения и конфигурации нового оборудования. Однако, если оборудование не поддерживает Plug and Play или не обнаруживается автоматически, вам придется сообщить о нем Windows 2000. Для этого нужно установить аппаратуру и соответствующие драйверы на систему при помощи мастера.

1. Запустите мастер установки и удаления оборудования, как описано выше, затем выберите Add/Troubleshoot A Device.
2. Щелкните Next (Далее). Windows 2000 будет искать новое оборудование для установки, а также имеющиеся устройства. Если новое оборудование не обнаруживается автоматически, выберите в списке пункт Add A New Device (Добавление нового устройства) и щелкните Next.
3. В окне Find New Hardware (Поиск нового оборудования) определите, должен ли мастер искать новое оборудование или вы хотите выбрать его из списка.
4. Если вы выберите Yes, мастер проведет тщательный поиск устройств и автоматически обнаружит новое оборудование. Процесс прохождения через все тины устройств

и параметры займет несколько минут. Когда поиск будет завершен, отобразятся все найденные новые устройства, и вы сможете выбрать нужное.

5. Если вы выберете No или если новые устройства не будут найдены автоматически, вам придется самим выбрать тип оборудования. Выберите тип оборудования, например, Modem (Модем) или Network Adapter (Сетевая плата), затем щелкните Next (Далее). Найдите в списке изготовителя устройства, а затем в списке справа выберите его модель.
6. Оставшиеся стадии процесса установки зависят от типа устанавливаемого устройства. Следуйте инструкциям и завершите установку, щелкнув Finish (Готово).

Удаление **оборудования**

Мастер можно использовать для удаления или отсоединения аппаратных устройств.

1. Запустите мастер установки и удаления оборудования, затем выберите Uninstall/Unplug A Device.
2. В диалоговом окне Choose A Removal Task (Выбор действия по удалению) отметьте, удаляете вы или отсоединяете устройство. При удалении устройства полностью удаляется устройство и его драйверы. При отсоединении — оно временно отключается.
3. Выберите устройство, которое хотите удалить или отсоединить.
4. Подтвердите, что вы хотите удалить или отсоединить устройство, выбрав Yes, I Want To Uninstall This Device (Удалить устройство) или Yes, I Want To Unplug This Device (Извлечь устройство).
5. Когда вы щелкнете Next (Далее), устройство будет удалено или отсоединено, Щелкните Finish (Готово) для завершения процесса.

Устранение неполадок оборудования и **устройств**

Мастер позволяет устранять неполадки оборудования.

1. Запустите мастер установки и удаления оборудования, затем выберите Add/Troubleshoot A Device.
2. В окне Choose A Hardware Device выберите устройство, неполадки которого нужно устранить. Щелкните Next.

3. В последнем окне мастера отображается состояние устройства. Когда вы щелкнете Finish (Готово), мастер сделает одно из двух: если в состоянии устройства — код ошибки, мастер откроет описание этого кода в интерактивной справке (если она доступна), иначе он запустит Hardware Troubleshooter, который пытается решить проблему, анализируя ваши ответы на вопросы.

Также можно прямо обращаться к Hardware Troubleshooter.

1. В консоли Computer Management (Управление компьютером) откройте Device Manager (Диспетчер устройств).
2. Устройства могут быть перечислены по типу, ресурсу или подключению. Щелкните правой кнопкой подключение устройства, неполадки которого хотите устранить, и выберите в контекстном меню Properties (Свойства). Откроется диалоговое окно свойств.
3. На кладке General (Общие) запустите Hardware Troubleshooter, щелкнув кнопку Troubleshooter (Устранение неполадок).

Глава 3

Мониторинг процессов, служб и событий

Ваша задача администратора сводится к обеспечению работы сетевых систем. Статус системных ресурсов и их использование могут радикально изменяться со временем, Службы могут прекращать работу. Файловым системам может не хватать места. Приложения могут выдавать исключения, что в свою очередь может вызывать проблемы с системой. Неавторизованные пользователи могут пытаться проникнуть в систему. Материалы этой главы помогут обнаружить и решить эти и другие проблемы с системой,

Управление приложениями, процессами и производительностью

При запуске приложения или вводе команды в командной строке Windows 2000 начинает один (или более) процесс, работая с соответствующей программой. Обычно процессы, запускаемые таким образом, называются *интерактивными*. То есть они запускаются *интерактивно — с* помощью клавиатуры или мыши. Если приложение или программа активны и выбраны, соответствующий интерактивный процесс контролирует клавиатуру и мышь, пока вы не переключите контроль, завершив работу программы или выбрав другую. Процесс, осуществляющий контроль, называют *активным*.

Процессы могут быть и *фоновыми*. В случае процессов, запускаемых пользователями, это означает, что программы, неактивные в данный момент, могут продолжать работу - только они. как правило, не обладают тем же приоритетом, что и активный процесс. Работу фоновых процессов можно настроить независимо от сеанса пользователя; такие процессы

обычно запускает ОС. Как пример такого типа фонового процесса можно привести командный файл, запускаемый командой AT. Последняя говорит системе запустить файл в определенное время, и при правильной настройке разрешений она отработает независимо от того, зарегистрирован ли пользователь в системе.

Диспетчер задач

Основной инструмент управления системными процессами и приложениями — Task Manager (Диспетчер задач) — открывается так;

- нажать Ctrl+Shift+Esc;
- нажать Ctrl+Alt+Del, затем выбрать кнопку Task Manager;
- набрать **taskmgr** в окне Run (Запуск программы) или в командной строке;
- щелкнуть правой кнопкой панель задач, затем выбрать Task Manager (Диспетчер задач) в контекстном меню.

Администрирование приложений

Вкладка Applications (Приложения) Диспетчера задач (рис. 3-1) показывает статус программ, работающих в данный момент в системе. Можно использовать кнопки в нижней части вкладки:

- остановить работу приложения, выбрав приложение, затем щелкнув End Task (Завершить задачу);
- перейти к приложению и сделать его активным, выбрав приложение, а затем щелкнув Switch To (Переключиться);
- запустить новую программу, выбрав New Task (Новая задача) и введя команду для запуска приложения; New Task выполняет ту же функцию, что и команда Run (Выполнить) в меню Start (Пуск).

Совет В столбце Status (Состояние) указано, нормально ли выполняется приложение или «зависло». Статус Not Responding (Не отвечает) — показатель того, что приложение, возможно, «зависло» и вам надо завершить связанные с ним задачи. Однако некоторые приложения могут не отвечать на запросы ОС в ходе выполнения интенсивных задач. Поэтому вы должны быть уверены, что приложение действительно «зависло», до того как завершить его.

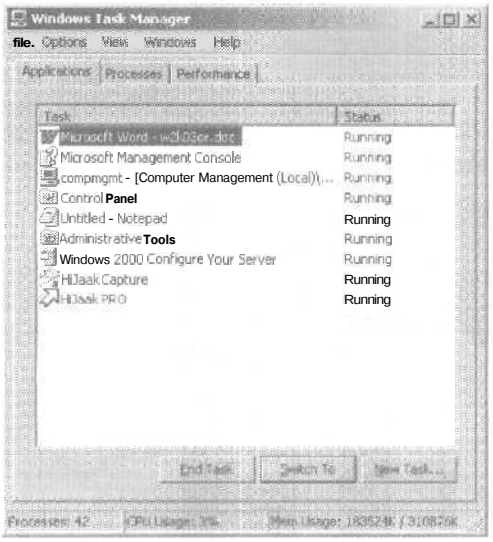


Рис. 3-1. Вкладка Applications в Task Manager показывает статус программ, работающих в **системе.**

Правый щелчок списка приложений

При правом щелчке этого списка отображается меню, позволяющее:

- **переходить** к приложению и делать **его активным;**
- **переводить** приложение на *передний* план;
- сворачивать и восстанавливать приложение;
- сворачивать или закрывать приложение;
- обращаться к процессу, связанному с этим приложением, показанному на вкладке Processes.

Примечание Команда **Go To** Process (Перейти к процессам) очень полезна, **когда** вы пытаетесь найти основной процесс для конкретного приложения. Выбор этой команды выделит соответствующий процесс на вкладке Processes.

Администрирование процессов

Подробная информация о выполняемых процессах дана на вкладке Process (Процессы) (рис. 3-2). При изучении процессов заметьте, что хотя у приложений есть основной про-

цесс, отдельное приложение может запускать несколько процессов. Обычно эти процессы зависят от главного процесса приложения и останавливаются при его прекращении или вызове команды End Task (Завершить задачу). Поэтому, как правило, предпочитают останавливать главный процесс приложения или само приложение, а не зависимые приложения.

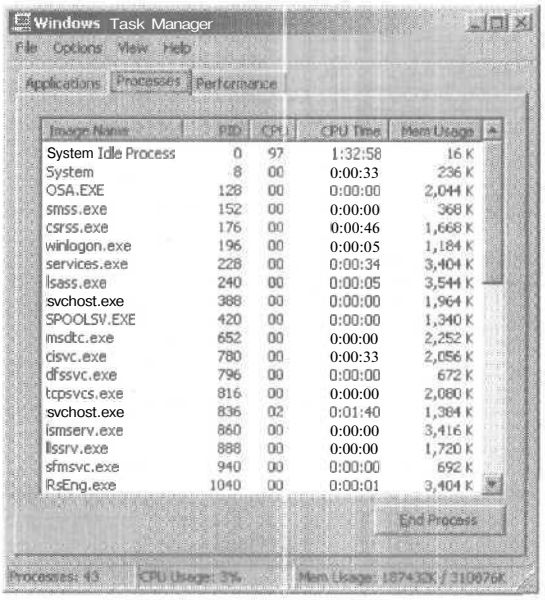


Рис. 3-2. Вкладка Processes дает подробную информацию о происходящих процессах.

Поля на вкладке Processes содержат информацию о выполняемых процессах, которая позволяет выявить процессы, поглощающие системные ресурсы, например, процессорное время и память. Эта вкладка также позволяет:

- остановить процесс, выбрав его, а затем — End Process (Завершить процесс);
- остановить процесс и его субпроцессы, щелкнув его правой кнопкой и выбрав End Process Tree (Завершить дерево процессов);
- настроить приоритет процесса, дважды щелкнув его, а затем выбрав Set Priority (Приоритет).

Примечание В списке процессов, выполняемых в Task Manager, вы заметите процесс System Idle Process (Бездействие системы). Нельзя задать приоритет этого процесса. В отличие от других процессов, отслеживающих использование ресурсов, System Idle Process отслеживает объем неиспользуемых ресурсов. Так, число 99 в столбце CPU (ЦП) означает, что 99% системных ресурсов не используется в настоящий момент.

Приоритет определяет, сколько системных ресурсов выделяется процессу. Большинство процессов обладает нормальным приоритетом по умолчанию. Для повышения приоритета надо сделать его высоким, для понижения — сделать его низким. Самый высокий приоритет отдается процессам, выполняемым в реальном времени.

Обзор производительности системы

Вкладка Performance (Быстродействие) отражает в виде графики и статистических данных степень использования процессора и памяти (рис. 3-3). Эта информация позволяет быстро оценить нагрузку на системные ресурсы. Чтобы получить более подробную информацию, используйте Performance Monitor, как показано ниже.

Графики на вкладке Performance

Графики на вкладке Performance дают следующую информацию:

- **CPU Usage** (Загрузка ЦП) — процент используемых ресурсов процессора;
- **CPU Usage History** (Хронология загрузки ЦП) — график истории нагрузки па процессор, составляемый с учетом времени;
- **MEM Usage** (Память) — объем памяти, используемой в настоящий момент на системе;
- **Memory Usage History** (Хронология использования памяти) — график истории использования памяти, составляемый с учетом времени.

Примечание Для просмотра крупного плана диаграмм дважды щелкните их. Повторный двойной щелчок вернет обычный режим просмотра.

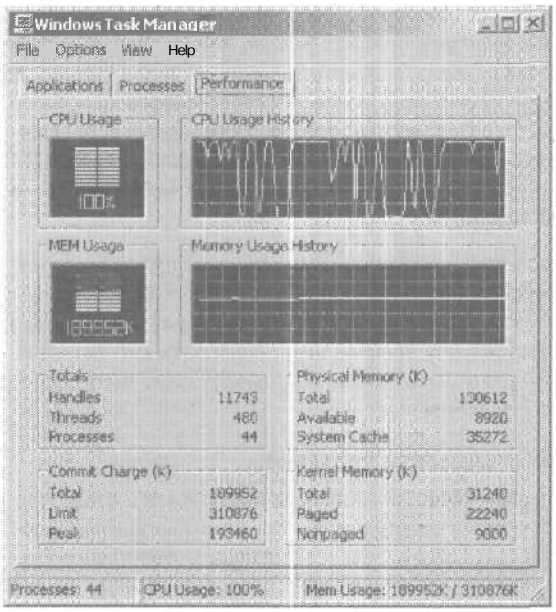


Рис. 3-3. Вкладка Performance позволяет быстро проверить использование системных ресурсов.

Настройка и обновление отображения графиков

Настроить или обновить отображения графиков помогут команды меню View (Вид):

- **Update Speed** (Скорость обновления) позволяет изменить скорость обновления графиков, а также приостановить обновление;
- **CPU History** (Загрузка ЦП) в многопроцессорных системах позволяет определить, как отображаются графики процессоров;
- **Show Kernel** Times (Вывод времени ядра) позволяет отобразить процессорное время, используемое ядром ОС.

Под графиками выведены следующие статистические данные.

- **Commit Charge** (Выделение памяти) — информация об общем объеме памяти, используемой ОС. В строке *Total* (Всего) отображается вся физическая и виртуальная память, используемая в данный момент, в строке *Limit* (Пре-

дел) — вся доступная физическая и виртуальная память, в строке *Peak* (Пик) — максимум памяти, использованной системой с момента загрузки.

- Kernel Memory (Память ядра) — информация о памяти, используемой ядром ОС. Значительные порции памяти ядра должны работать в оперативной памяти и не могут подкачиваться в виртуальную память. Такой тип памяти ядра отображается как *Nonpaged* (Невыгружаемая). Остальная часть памяти ядра может подкачиваться в виртуальную память и отображается как *Paged* (Выгружаемая). Общий объем памяти, используемой ядром, приводится в строке *Total.*
- Physical Memory (Физическая память) — информация об общем объеме оперативной памяти в системе. *Total* — объем физической оперативной памяти. *Available* (Доступно) — оперативная память, не используемая в данный момент. *System cache* (Системный кэш) — память, используемая ОС для кэширования.
- Totals (Всего) — информация о нагрузке на процессор. *Handles* (Дескрипторов) — количество используемых дескрипторов ввода-вывода, *Threads* (Потоков) — потоков, *Processes* (Процессов) — процессов.

Управление системными службами

Службы предоставляют ключевые функции рабочим станциям и серверам Windows 2000. Для управления системными службами служит программа Services (Службы) из консоли Computer Management (Управление компьютером), которая открывается так.

1. Start\Programs\Administrative Tools\Computer Management (Пуск\Программы\Администрирование\Управление компьютером). Или выберите Computer Management R папке Administrative Tools.
2. Щелкнув правой кнопкой Computer Management в дереве консоли, выберите Connect To Another Computer (Подключиться к другому компьютеру). Теперь можно выбрать систему, службами которой вы хотите управлять.
3. Откройте узел Services And Applications (Службы и приложения), щелкнув значок (+) рядом с ним, затем выберите Services (Службы).

Примечание В Windows 2000 предусмотрены и другие способы доступа к слухбам, например, через элемент Services в приложении Component Services (Службы компонентов).

Взгляните на узел Services (Службы) в консоли Computer Management (рис. 3-4). Ключевые поля этого диалогового окна используются следующим образом.

- Name (Имя) — имя службы. Здесь перечислены только службы, установленные в системе. Дважды щелкните имя службы, чтобы задать параметры ее запуска. Если нужной службы нет в списке, ее можно установить из окна свойств сетевого подключения или вызвав мастер Windows Optional Networking Components (см. главу 15).
- Description (Описание) — краткое описание службы и ее назначения.
- Status (Состояние) -- служба работает, приостановлена или остановлена (для остановленной службы столбец пуст).

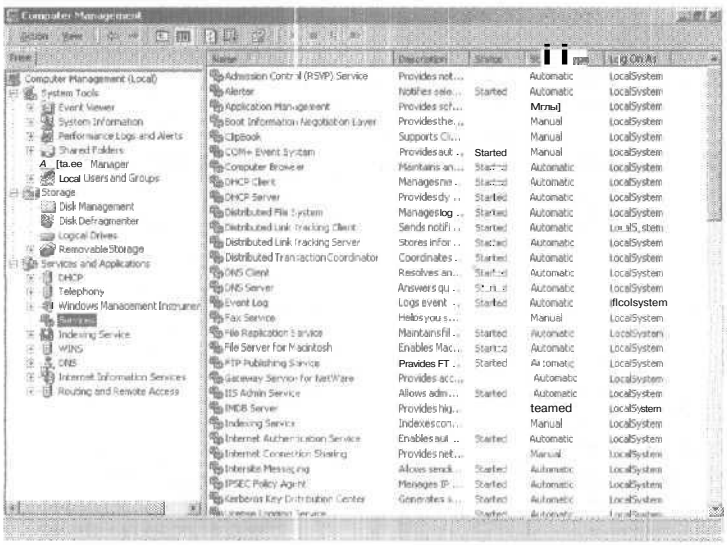


Рис. 3-4. Узел Services служит для управления рабочими станциями и серверами Windows 2000.

- Startup Type (Тип запуска) — параметры запуска службы. Автоматические службы запускаются при загрузке системы. Ручные службы запускаются пользователями или другими службами. Отключенные устройства выключаются и не могут запускаться, пока остаются отключенными.
- Log On As (Вход в систему) — учетная запись, под которой служба входит в систему. Обычно по умолчанию используется локальная учетная запись системы.

Примечание И ОС, и пользователи могут отключать службы. Обычно Windows 2000 отключает службу, если возникает конфликт с другой службой.

Стандартные службы Windows 2000

Ниже перечислены стандартные службы, которые можно увидеть на системах Windows 2000 (табл. 3-1). Помните: тип и количество выполняемых служб зависит от конфигурации. Для установки или удаления служб предназначено средство Configure Your Server (Настройка сервера).

Табл. 3-1. Стандартные службы, которые можно установить на системы Windows 2000.

Имя службы	Описание
Alerter	**Отправляет** административные сигналы оповещения.
Application Management	Службы установки ПО.
ClipBook	Удаленный просмотр локальных страниц при помощи ClipBook Viewer.
COM+ Event System	Автоматически распространяет события COM-компонентам — подписчикам.
Computer Browser	Обзор компьютера; поддерживает список ресурсов, используемых для сетевого обзора.
Dynamic Host Configuration Protocol (DHCP) Client	Управляет конфигурацией сети путем регистрации и обновления IP-адресов и DNS-имен.
DHCP Server	Распределяет динамические IP-адреса и сетевой конфигурацией для DHCP-клиентов.
Distributed Transaction Coordinator	Координирует распределенные транзакции для диспетчеров ресурсов.
DNS Client	Разрешает и кэширует DNS-имена.

Табл. 3-1. *(продолжение)*

Имя службы	Описание
DNS Server	Управляет DNS-именами и запросами.
Event Log	Заносит в журнал сообщения о событиях, вьдаваемых приложениями и ОС. .
File Server for Macintosh	Позволяет пользователям Macintosh хранить и открывать файлы на системе сервера.
Gateway Service for NetWare	Доступ к ресурсам файлов и принтеров в сетях NetWare.
Intersite Messaging	Отправляет и получает сообщения между узлами Active Directory.
License Logging Service	Отслеживает использование лицензий и совместимость.
Messenger	Отправляет и получает сообщения, передаваемые администраторами или службой Alerter.
Net Logon	Аутентифицирует вход пользователя.
Network dynamic data exchange (DDE)	Поддерживает DDE между приложениями.
Network DDE DSDM	Угравляет обменом разделяемых динамических данных и используется Network DDE.
NT LM Security Support Provider	Обеспечивает безопасность RPC-программ, не использующих именованные каналы.
Performance Logs and Alerts	Конфигурирует журналы производительности и сигналы оповещения.
Plug and Play	Управляет установкой и **конфигурацией** устройств, а также уведомляет программы об изменениях в устройствах.
Print Server for Macintosh	Позволяет пользователям Macintosh отправлять задание на печать в Windows.
Print Spooler	Организует очередь печати.
Protected Storage	Защищенное хранилище для важных данных, например личных ключей.
RPC	RPC-службы для распределенных приложений.
RPC Locator	Управляет базой данных служб имен RFC.
Routing and Remote Access	Службы удаленного доступа и маршрутизации.

Табл. 3-1. *(продолжение)*

Имя службы	Описание
Secondary Logon Service	Обеспечивает функцию Run As (Запуск от имени), чтобы выполнять процессы от имени другого пользователя.
Security Accounts Manager	Хранит информацию о безопасности для локальных учетных записей пользователей.
Server	Службы RPC-сервера, включая разделение файлов, очередь печати и именованные каналы.
Simple Transmission Control Protocol/Internet Protocol (TCP/IP) Services	Поддерживает службы TCP/IP Character Generator, Daytime, Discard, Echo и Quote of the Day.
System Event Notification	Отслеживает события системы и уведомляет абонентов COM+ Event System об этих событиях.
Task Scheduler	Планировщик работ.
TCP/IP NetBIOS Helper Service	Поддержка NetBIOS поверх TCP/IP и разрешение имен в NetBIOS.
Telnet	Позволяет удаленному пользователю входить в систему и выполнять консольные программы из командной строки.
Windows Internet Name Service (WINS)	Предоставляет службу имен NetBIOS для TCP/IP-клиентов.
Workstation	Предоставляет службы для сетевых соединений и коммуникаций.

Запуск, остановка и приостановка служб

Вам часто придется запускать, останавливать или приостанавливать службы Windows 2000. Для этого сделайте так.

1. Откройте консоль Computer Management.
2. Щелкнув правой кнопкой Computer Management в дереве консоли, выберите Connect To Another Computer. Теперь можно выбрать систему, службами которой вы собираетесь управлять.
3. Раскройте узел Services And Applications, щелкнув значок (+) рядом с ним, затем выберите Services.
4. Щелкнув правой кнопкой службу, которой собираетесь управлять, затем Start (Пуск), Stop (Стон) или Pause

(Пауза). Также можно выбрать Restart (Перезапуск): Windows остановит службу и после короткой паузы запустит ее снова. Кроме того, если вы делаете паузу в работе службы, можете выбрать команду Resume (Продолжение) для возобновления ее работы.

Примечание Когда службы не могут запуститься автоматически, состояние не отображается, и обычно выдается уведомление во всплывающем диалоговом окне. Сбои служб также могут регистрироваться в журналах событий системы. В Windows 2000 можно настроить действия на случай сбоя в запуске службы. Например, Windows 2000 может попытаться перезапустить службу. Подробнее об этом см. раздел «Конфигурация восстановления службы».

Конфигурация запуска службы

Службы Windows 2000 можно настроить для ручного или автоматического запуска, а также вообще выключить.

1. В консоли Computer Management установите соединение с компьютером, службами которого хотите управлять.

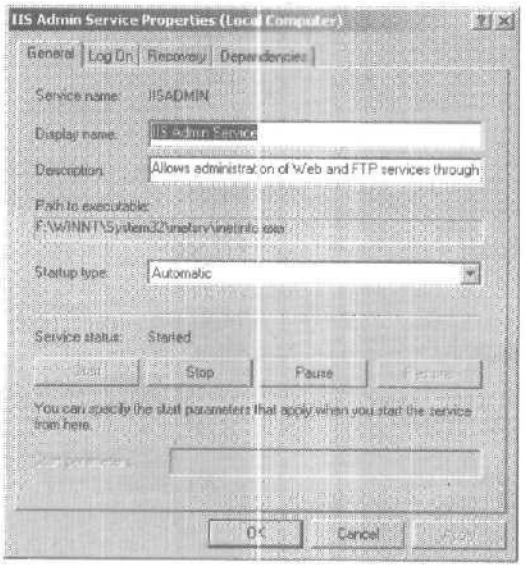


Рис. 3-5. Список Startup на вкладке General позволяет конфигурировать параметры запуска службы.

2. Откройте узел Services And Applications, щелкнув значок (+) рядом с ним, затем выберите Services.
3. Щелкнув правой кнопкой службу, которую собираетесь конфигурировать, выберите Properties.
4. На вкладке General (Общие) в списке Startup Type (Тип запуска) выберите параметры запуска (рис. 3-5). Выберите Automatic (Авто), чтобы запустить службы при загрузке, Manual (Вручную) — чтобы запускать службы вручную, или Disabled (Отключено) — чтобы отключить службу.
5. Щелкните OK.

Конфигурация регистрации службы

Службы Windows 2000 можно настроить для входа под учетной записью системы или конкретного пользователя.

1. В консоли Computer Management установите соединение с компьютером, службами которого собираетесь управлять.
2. Откройте узел Services And Applications, щелкнув значок (+) рядом с ним, затем выберите Services.

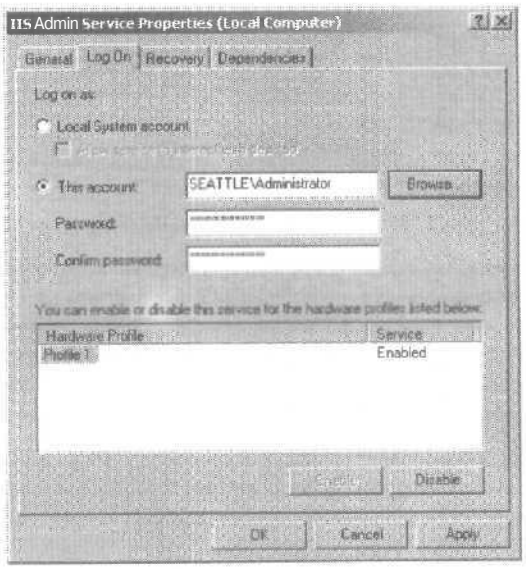


РИС. 3-6. Вкладка Log On служит для конфигурации учетной записи службы.

3. Щелкнув правой кнопкой службу, которую собираетесь конфигурировать, выберите Properties.
4. Перейдите на вкладку Log On (Вход в систему) (рис. 3-6).
5. Выберите Local System Account (С системной учетной записью), если служба должна регистрироваться под учетной записью системы (по умолчанию для большинства служб).
6. Выберите This Account (С учетной записью), если служба регистрируется под учетной записью конкретного пользователя. Наберите в полях имя учетной записи и пароль. Кнопка Browse (Обзор) служит для поиска учетной записи пользователя.
7. Щелкните OK.

Конфигурация восстановления службы

Можно настроить службы Windows 2000, чтобы они выполняли определенные действия в случае своего сбоя. Например, можно перезапустить службу или выполнить приложение. Чтобы сконфигурировать параметры восстановления службы, сделайте следующее.

1. В консоли Computer Management установите соединение с компьютером, который собираетесь управлять.
2. Откройте узел Services And Applications, щелкнув значок (+), затем выберите Services.
3. Щелкнув правой кнопкой службу, которую собираетесь конфигурировать, выберите Properties (Свойства).
4. Выберите вкладку Recovery (Восстановление) (рис: 3-7).

Примечание Windows 2000 автоматически конфигурирует восстановление для некоторых важных системных служб при установке. На рис. 3-7 видно, что IIS (Internet Information Server) Admin Service настроена для выполнения программы, устраняющей проблемы в службе и безопасно управляющей зависимыми IIS-службами при перезапуске службы.

5. Теперь можно конфигурировать параметры восстановления для первого, второго и дальнейших сбоев восстановления. Доступны следующие параметры:
   - Take No Action (Ничего не делать);
   - Restart the Service (Перезапуск службы);

- Run a File (Выполнение программы);
- Reboot the Computer (Перезагрузка компьютера).

Совет При конфигурации параметров восстановления для важных служб можно перезапустить службу на первой и второй попытках, а на третьей — перезагрузить сервер.

6. Задайте другие параметры, основываясь на выбранных параметрах восстановления. Если вы решили выполнить программу, задайте параметры в области Run File. Если вы решили перезапустить службу, определите задержку перезапуска. После остановки службы Windows 2000 ждет в течение указанного срока до попытки запустить службу. Обычно достаточно подождать 1-2 минуты.
7. Щелкните OK.

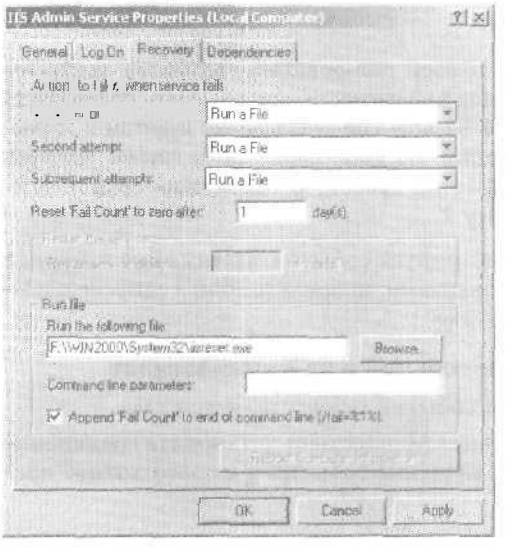


Рис. 3-7. Вкладка Recovery позволяет определить действия на случай сбоя службы.

Запись в журнал и просмотр события

Журналы событий хранят хронологическую информацию, помогающую выявить проблемы в системе и безопасности. Служба записей событий в журнал контролирует, отслежи-

ваются ли события на системах Windows 2000. Когда эта служба запущена, вы можете отследить действия пользователя и события обращения к системным ресурсам по следующим журналам событий:

- **Application Log** регистрирует события, записанные в журнал приложениями, например сбой MS SQL при доступе к базе данных;
- **Directory Service** регистрирует события, записанные в журнал Active Directory и относящимися к ней службами;
- **DNS Server** регистрирует очереди, ответы DNS, а также другие действия DNS;
- **File Replication Service** регистрирует репликацию файлов;
- **Security Log** регистрирует события, настроенные для аудита, выполняемого посредством локальной или групповой политики;

Примечание Любой пользователь, которому требуется доступ к журналу безопасности, должен иметь право Manage Auditing And Security Log (Управление аудитом и журналом безопасности). По умолчанию члены группы Administrators обладают этим правом, О присвоении прав пользователя см. главу 7.

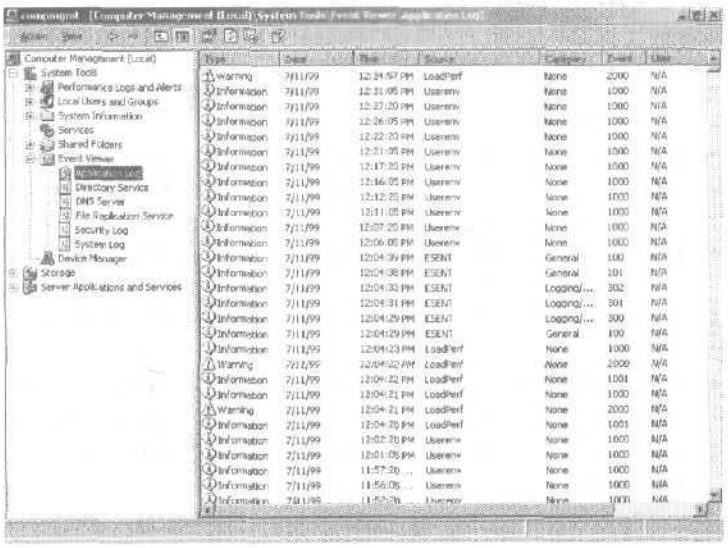
- **System Log** регистрирует события, записанные в журнал ОС или ее компонентами; например, сбой в запуске службы при перезагрузке.

Доступ к журналам событий и их использование

Доступ к журналам событий осуществляется так.

1. В консоли Computer Management установите соединение с компьютером, журналы событий которого хотите просмотреть.
2. Откройте узел System Tools, щелкнув значок (+) рядом с ним и затем дважды щелкнув Event Viewer. Появится список журналов (рис. 3-8).
3. Выберите журнал, который хотите просмотреть.

Элементы в главной панели Event Viewer позволяют быстро просмотреть, когда, где и как произошло событие. Чтобы получить подробную информацию о событии, дважды щел-



Рис, 3-8. Event Viewer отображает события для выбранного журнала.

кните **его запись. После** типа события обозначены его дата и **время. Типы** событий:

- **Information** — информационное событие, как правило, связанное с успешным действием;
- **Success Audit** — событие, связанное с успешным выполнением действия;
- Failure **Audit** — событие, связанное со сбоем в выполнении действия;
- **Warning** — предупреждение; подробности в предупреждениях часто бывают полезны для предотвращения будущих проблем с системой;
- **Error** — ошибка, например, неудачный запуск службы.

Примечание Предупреждения и ошибки — два типа событий, которым следует уделить особое внимание. Когда происходят такие события и вы не уверены в их причине, щелкните дважды элемент для обзора подробного описания события.

Помимо типа, даты и времени, общие и **подробные записи** событий предоставляют следующую **информацию:**

- Source — приложение, служба или компонент, записавший событие;
- Category — категория события, иногда используемая для дальнейшего описания связанного с ним действия;
- **Event** — определяет конкретное событие;
- **User** — учетная запись пользователя, **действовавшая** *в* момент события;
- Computer — имя компьютера, на котором произошло событие;
- Description — в подробных записях — текстовое описание события;
- Data — в подробных записях — любые данные или код ошибки, выданные событием.

Настройка параметров журнала событий

Параметры журнала позволяют контролировать размер и ведение журналов событий. По умолчанию максимальный размер файлов журналов событий — 512 Кб. Когда размер журнала выходит за этот предел, события старше 7 дней переписываются, чтобы максимальный размер файла не превышался.

Параметры журнала устанавливают так,

1. В консоли Computer Management щелкните дважды элемент Event Viewer. Появится список записей событий.
2. Щелкнув правой кнопкой журнал событий, параметры которого хотите установить, выберите Properties в контекстном меню. Откроется диалоговое окно (рис. 3-9).
3. Введите максимальный размер в поле Maximum Log Size. Убедитесь, что на диске, содержащем ОС, хватает свободного места для выбранного вами максимального размера журнала. По умолчанию файлы журналов хранятся в каталоге *%SystemRoot%*\system32\config.

Примечание В этой книге часто упоминается о *%SystemRoot%*. Эта переменная окружения используется Windows 2000 для обозначения базового каталога ОС Windows 2000, например C:\WIN2000. О переменных окружения см. главу 9.

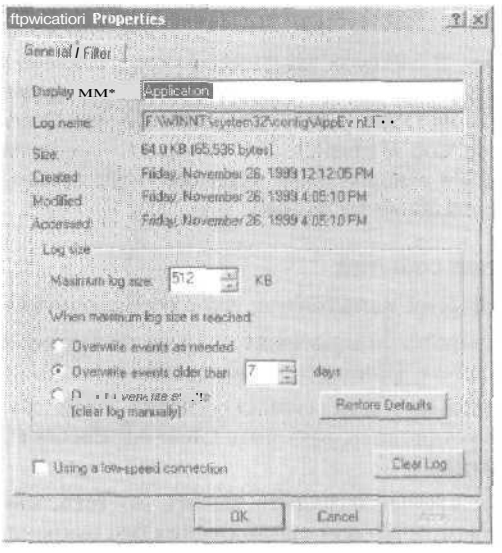


Рис. 3-9. Конфигурируйте параметры журнала в соответствии с уровнем аудита в системе.

4. Определите результат достижения максимального размера журнала.

   - Overwrite Events As Needed (Затирать старые события по необходимости) — события в журнале переписываются при достижении максимального размера файла. Обычно это оптимальный параметр на системе с низким приоритетом.
   - Overwrite Events Older Than *X* Days (Затирать события старее *X* дней) — при достижении максимального размера файла события в журнале переписываются, только если они старше выбранного параметра. Если достигается максимальный размер и события не могут быть переписаны, система выдает сообщение об ошибке, говоря, что журнал событий переполнен.
   - **Do Not Overwrite Events (Clear Log Manually) [Не** затирать события (очистка журнала вручную)] — при достижении максимального размера файла система сообщает об ошибке, отмечая, что журнал событий переполнен.

5. Щелкните OK, когда завершите.

Примечание В системах, где безопасность и ведение журналов событий очень важны, можно определить параметры Overwrite Events Older Than *X* Days или Do Not Overwrite Events (Clear Log Manually). Это позволит периодически архивировать и очищать файл журнала, чтобы система не выдавала сообщений об ошибке.

Очистка журналов событий

Когда журнал событии наполнится, его следует очистить.

1. В консоли Computer Management дважды щелкните элемент Event Viewer. Появится список записей событий.
2. Щелкнув правой кнопкой журнал событий, свойства которого хотите установить, выберите Clear All Events (Стереть все события).
3. Выберите Yes, чтобы сохранить записи до того, как ее очистить. Выберите No для продолжения без сохранения файла журнала.

Архивирование журналов событий

На некоторых ключевых системах, таких как контроллеры домена и серверы приложений, требуется, чтобы журналы сохранялись несколько месяцев. Но обычно для этого не принято устанавливать максимальный размер журналов. Вместо этого периодически архивируют журналы событий.

Форматы архивов журналов

Журналы можно архивировать в трех форматах:

- формат журнала событий для доступа в Event Viewer;
- формат текста с разделением табулятором для доступа в текстовых редакторах или импорта в электронные таблицы и БД;
- формат текста с разделением запятыми для импорта в электронные таблицы или БД.

При экспорте файлов журнала в файл с разделением запятыми, каждое поле в записи события отделяется запятой. Записи событий выглядят так:

```
9/7/99,9:43:24PM,DNS,Information,None,2,N/A,ZETA,The DNS
Server has started.
```

9/7/99,9:40:04PM,DNS,Error,None,4015,N/A,ZETA,The DNS server has encountered a critical error from the Directory Service CDS). The data is the error code.

Формат записей таков:

дата, время, источник, тип, категория, событие, пользователь, компьютер, описание.

Создание архивов журналов в формате Event Viewer

Архив журнала в файловом формате Event Viewer создается так.

1. В консоли Computer Management дважды щелкните Event Viewer. Появится список журналов событий.
2. Щелкнув правой кнопкой журнал событий, который хотите архивировать, выберите Save Log File As (Сохранить файл журнала как).
3. В окне Save As выберите каталог и имя файла журнала.
4. В окне Save As типом файла по умолчанию будет Event Log (*.evt).
5. Щелкните Save.

Примечание **Чтобы** регулярно архивировать журналы, создайте **каталог** архивов. **Это облегчит** поиск архивов журналов. Файлу журнала надо дать такое имя, чтобы можно было определить тип файла журнала и время архивирования. Скажем, если вы архивируете системный файл журнала января 2000 г., можете использовать имя файла System **Log Jan. 2000.**

Создание журналов архивов в других форматах

Архив журнала с разделением запятыми или табуляторами создается так.

1. В консоли Computer Management дважды щелкните элемент Event Viewer. Появится список журналов событий.
2. Щелкнув правой кнопкой журнал событий, который хотите архивировать, выберите Save Log File As из контекстного меню.
3. В диалоговом окне Save As выберите каталог и имя файла журнала.

4. В списке Save As Type выберите формат **файла** журнала Text **или CSV.**
5. Щелкните **Save.**

Просмотр архивов журналов

Архивы журналов можно просматривать в текстовом формате в любом текстовом редакторе. Чтобы просмотреть архивы журналов в Event Viewer (Просмотр событий), сделайте так.

1. В консоли Computer Management щелкните правой кнопкой элемент Event Viewer. В контекстном меню выберите Open Log File. Откроется диалоговое окно Open (Открыть) (рис. 3-10).
2. Выберите каталог и имл файла.
3. Выберите тип файла журнала, затем введите отображаемое имя журнала.
4. Введите отображаемое имя файла журнала.
5. Щелкните Open. Архивированный журнал появится в виде отдельного окна в Event Viewer. Выберите это окно для отображения сохраненных событий в журнале.

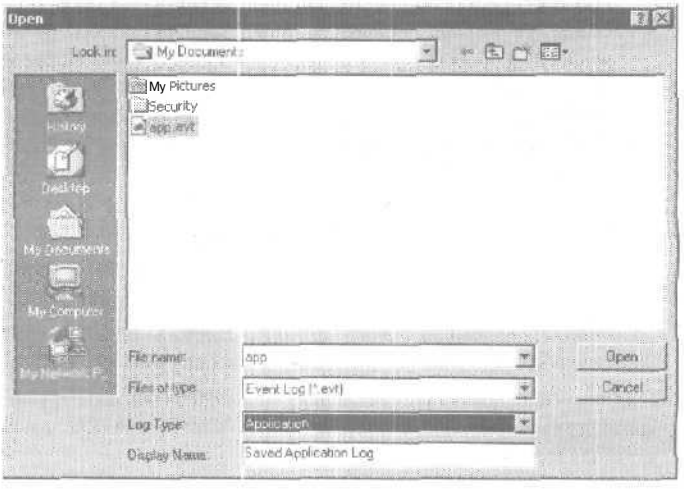


Рис. 3-10. Диалоговое окно Open служит для открытия сохраненного журнала события в новом окне.

Мониторинг производительности и действий сервера

Мониторинг сервера следует производить обдуманно и по плану.

Для чего нужен мониторинг

Устранение неполадок в производительности сервера — главная причина мониторинга. Например, мониторинг сервера может понадобиться для устранения проблем пользователей с подключением к серверу.

Еще одна типичная причина мониторинга сервера — повышение производительности сервера. Это делается путем оптимизации дисковых операций, снижения нагрузки на процессор и сокращения нагрузки сетевого трафика на сервер. К сожалению, это часто оказывается платой за ресурсы. Например, по мере возрастания количества пользователей, получающих доступ к серверу, вы можете быть не в состоянии сократить нагрузку сетевого трафика, но вы можете улучшить производительность сервера, балансируя нагрузку или распределяя ключевые файлы данных по отдельным дискам.

Подготовка к мониторингу

До начала мониторинга следует выяснить метрику основной производительности сервера. Для этого его производительность измеряется в разные моменты времени и при разных условиях нагрузки. Затем можно сравнить основную производительность с последующей производительностью, чтобы выяснить, как работает сервер. Метрика производительности, превышающая основные измерения, может указывать на те области, где сервер следует оптимизировать или конфигурировать заново.

После установки основной метрики составляется план мониторинга. В подробный план включите следующие этапы.

1. Определите, какие события сервера требуют мониторинга для достижения наших целей.
2. Установите фильтры для сокращения количества собираемой информации.
3. Настройте мониторы и сигналы оповещения для отслеживания событий.

4. Запишите данные о событии в журнал.
5. Проанализируйте данные о событии в Performance Monitor.

Хотя в большинстве случаев следует вырабатывать план мониторинга, иногда не обязательно проходить все стадии. Например, может требоваться мониторинг и анализ по ходу действий, а не запись в журнал и анализ данных позже.

Использование Performance Monitor

Performance Monitor (Монитор производительности) графически отображает статистику для ряда выбранных параметров производительности, называемых *счетчиками*. Доступные счетчики можно обновлять и при установке служб и дополнений на сервер. Например, при конфигурации DNS на сервере, Performance Monitor пополняется рядом объектов и счетчиков для отслеживания производительности DNS.

Performance Monitor создает график с отслеживаемыми счетчиками. Интервал обновления для этого графика конфигурируется, но по умолчанию устанавливается на 1 секунду. Работая с Performance Monitor, вы увидите, что информация отслеживания наиболее ценна при записи данных в файл журнала, при конфигурации сигналов оповещения для отправки сообщений, когда происходят определенные события или когда достигаются определенные пороги, например, процессорное время — 99%.

Выбор счетчиков для мониторинга

Performance Monitor отображает информацию только для отслеживаемых счетчиков. Доступно множество счетчиков, а по мере добавления служб их становится больше. Счетчики организованы в группы — *объекты производительности*. Например, все счетчики, связанные с процессором, связаны и с объектом Processor.

Счетчики выбираются так.

1. Выберите Performance (Производительность) в меню Administrative Tools. Появится консоль Performance.
2. Выберите элемент System Monitor в левой панели (рис. 3-11).
3. У Performance Monitor несколько режимов просмотра. Для включения режима диаграммы щелкните кнопку View Chart (Просмотр диаграммы) в панели инструментов.

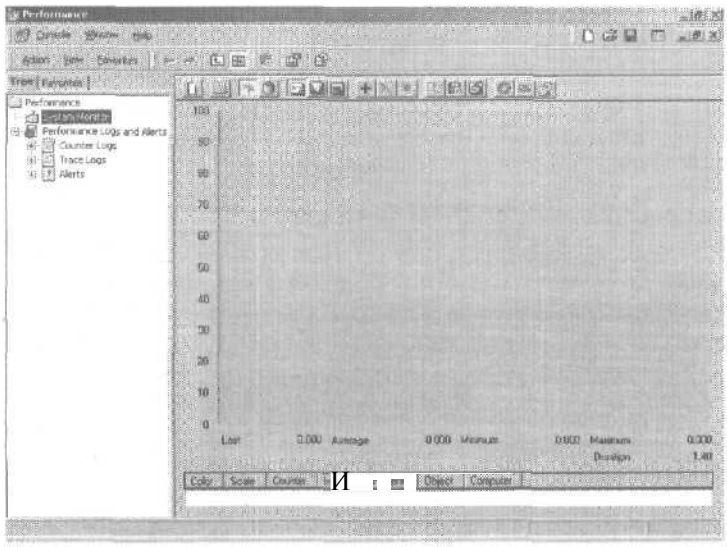


Рис. **3-11.** Счетчики отображаются в нижней части окна Performance Monitor.

4. Чтобы добавить счетчики, щелкните кнопку Add (Добавить) в панели инструментов. Появится диалоговое окно Add Counters (Добавить счетчики) (рис. 3-12). Вот его основные поля;
   - **Use Local Computer Counters** (Использовать локальные счетчики) — конфигурация параметров производительности локального компьютера;
   - Select **Counters From Computer** (Выбрать счетчики с компьютера) — введите UNC-имя сервера, с которым собираетесь работать, например \\ZETA, или выберите сервер в списке доступных по сети компьютеров;
   - **Performance Object** (Объект) — выберите тип объекта, с которым собираетесь работать, например Processor;

Примечание Изучите объекты и счетчики в окне Add Counters. Выберите объект в списке Performance Object, щелкните кнопку Explain (Объяснение), затем прокрутите список счетчиков для этого объекта.

   - **All Counters** (Все счетчики) — выберите все счетчики для текущего объекта;

- **Select Counters** From **List** (Выбрать счетчики из списка) — выберите один или более счетчиков для текущего объекта, например % Processor Time и % User Time;
- All **Instances** (Все вхождения) — выберите все экземпляры счетчиков для мониторинга;
- Select **Instances; From List** (Все вхождения из списка) — выберите один или более экземпляр счетчика для мониторинга.

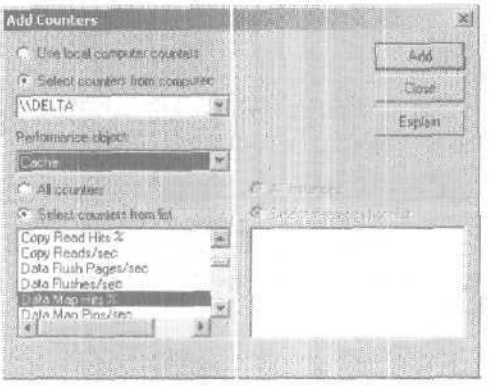


Рис. 3-12. Выберите счетчики для мониторинга.

Совет Не выбирайте слишком много счетчиков или их экземпляров одновременно. Графики будет сложно читать, и вы повысите нагрузку на ресурсы системы — а именно процессорное время *л* память — это может замедлить время отклика сервера.

5. Выбрав нужные параметры, щелкните Add (Добавить), чтобы добавить счетчики в график. Затем повторите этот процесс, чтобы добавить другие параметры производительности.
6. Щелкните Done (Закрыть), когда завершите добавление счетчиков.
7. Позже счетчики можно удалить, щелкнув их элемент в нижней части окна Performance, а затем Delete (Удалить).

Журналы производительности

Журналы производительности позволяют отслеживать производительность сервера. Параметры, отслеживаемые в файлах журналов, записываются отдельно от параметров, отображаемых на графике в окне Performance. Можно настроить файлы журнала для обновления данных счетчика автоматически или вручную. В первом случае снимок ключевых параметров записывается в определенные интервалы времени, например каждые 10 с. Во втором — вы сами определяете, когда делать снимки. Доступны два типа журналов производительности:

- **Counter Logs** (Журналы счетчиков) — сюда записываются данные о производительности выбранных счетчиков по истечении заданного интервала обновления;
- **Trace Logs** (Журналы трассировки) — сюда записываются данные о производительности всякий раз, когда происходят события, связанные с ней.

Создание и управление журналами производительности

Журналы производительности создаются так.

1. Откройте консоль Performance, выбрав Performance в меню Administrative Tools.
2. Раскройте узел Performance Logs And Alerts (Оповещения и журналы производительности), щелкнув рядом с ним значок (+). Если вы собираетесь конфигурировать счетчик, выберите Counter Logs (Журналы счетчиков); иначе выберите Trace Logs (Журналы трассировки).
3. В правой панели появится список текущих журналов (рис. 3-13), Зеленый значок указывает, что журнал в настоящий момент регистрирует данные; красный — что регистрация данных приостановлена.
4. Можно создать новый журнал, щелкнув правой кнопкой в правой панели и выбрав в контекстном меню New Log Settings. Появится окно New Log Settings (Новые параметры журнала), где нужно задать описательное имя для новых параметров журнала.
5. Для управления существующим журналом щелкните правой кнопкой его элемент в правой панели и выберите один из следующих параметров:
   - Start — для активизации журнала;

- **Stop** — для остановки журнала;
- **Delete** — для удаления журнала;
- **Properties** — для отображения окна свойств журнала.

Рис. 3-13. Текущие журналы производительности перечислены с обобщающей информацией.

Создание журналов счетчиков

В журналах счетчиков регистрируются данные производительности выбранных счетчиков через определенный интервал времени. Например, можно собирать данные о производительности процессора каждые 15 минут. Журнал счетчика создается так.

1. Выберите Counter Logs в правой панели консоли Performance, затем в правой панели щелкните правой кнопкой и выберите New Log Settings.
2. В диалоговом окне New Log Settings наберите имя журнала, например System Performance Monitor или Processor Status Monitor, и щелкните OK.
3. На вкладке General щелкните Add, чтобы вывести диалоговое окно Select Counters; оно похоже на окно Add Counters (рис. 3-12).

4. В диалоговом окне Select Counters (Выбор счетчиков) добавьте счетчики для записи в журнал. Щелкните Close, когда закончите.
5. В поле Sample Data Every... (Сжимать показания каждые) наберите интервал сжатия и выберите единицу времени и секундах, минутах, часах или днях. Интервал сжатия определяет, когда собираются новые данные. Например, при сжатии каждые 15 минут журнал обновляется каждые 15 минут.
6. Щелкните вкладку Log Files (рис. 3-14) и определите, как создавать файл журнала, используя следующие поля,
   - **Location** (Размещение) задает место для файла журнала.
   - **File Name** (Имя файла) задает имя файла журнала.
   - **End File Names With** (Дописывать к имени) — задает автоматический суффикс для каждого нового файла, создаваемого при выполнении журнала счетчика. Журналы могут иметь цифровой суффикс или суффикс в особом формате данных.

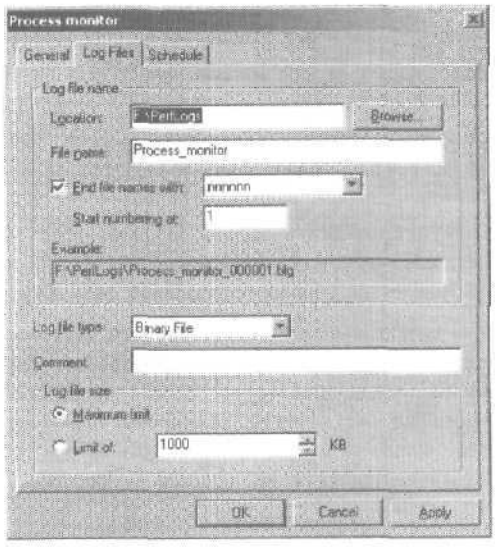


Рис. 3-14. Конфигурируйте формат и использование файла журнала.

- **Start** Numbering At (Начать нумерацию с) задает первое серийное число для журнала, использующего автоматический числовой суффикс.
- Log File **Type** (Тип журнала) задает тип создаваемого файла журнала. Используйте Text File — CSV (Текстовый файл — CSV) для файла журнала с разделением запятыми, Text File — TSV (Текстовый файл - TSV) — для файла журнала с разделением табулятором, Binary File (Двоичный файл) — для создания двоичного файла, который можно читать при помощи Performance Monitor, а Binary Circular File (Двоичный циклический файл) - для создания двоичного файла, записывающего новые данные поверх старых, когда размер файла достигает определенного предела.

Совет Если вы планируете использовать Performance Monitor для анализа или просмотра журнала, используйте один из форматов двоичного файла.

- **Comment** (Комментарий) задает дополнительное описание журнала, отображаемое в столбце Comment.
- **Maximum Limit** (Максимально возможный) не задает предустановленного предела размера файла журнала.
- **Limit Of** (Не более) задает конкретный предел в кб для размера файла журнала.

7. Щелкните вкладку Schedule (Расписание) (рис. 3-15), затем определите, когда запись в журнал должна начинаться и кончаться.
8. Вы можете сконфигурировать запуск журнала вручную или автоматически в определенное время. Выберите подходящий параметр и если нужно, определите дату запуска,

Совет Файлы журнала могут быстро вырасти. Если вы хотите регистрировать данные в течение длительного времени, убедитесь, что поместили журнал файла на достаточно емкий диск. Помните: чем чаще вы обновляете файл журнала, тем больше моста будет на диске и тем эффективнее будет использование ресурсов процессора на системе.

9. Можно сконфигурировать остановку файла журнала:
   - вручную;

- ЕЮ истечении определенного периода времени, например, семи дней;
- в определенный день и время;
- когда файл журнала будет заполнен (если ограничить размер файла).

10. Щелкните OK, когда закончите настройку расписания журнала. Будет создан журнал, и им можно будет управлять (см. раздел «Создание и управление журналом производительности»).

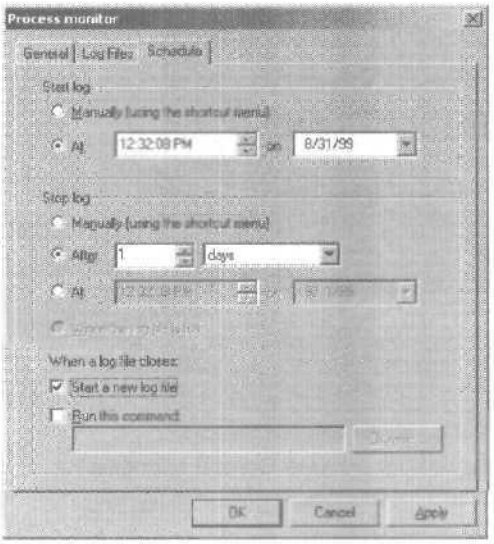


Рис. 3-15. Определите, когда начинается и кончается регистрация данных.

Создание журналов трассировки

Журналы трассировки записывают данные о производительности, когда происходят события для их поставщиков источников. Поставщик источника — это приложение или служба ОС, обладающая трассируемыми событиями. На контроллерах домена можно найти двух поставщиков источников: это сама ОС и Active Directory:NetLogon. На других серверах ОС будет единственным доступным поставщиком.

Журнал трассировки создается так.

1. Выбрав Trace Logs в левой панели консоли Performance, щелкните правой кнопкой в правой панели. В контекстном меню выберите New, а затем — New Log Settings.
2. В диалоговом окне New Log Settings наберите имя журнала, например Logon Trace или Disk I/O Trace, и щелкните OK. Откроется такое окно (рис. 3-16):

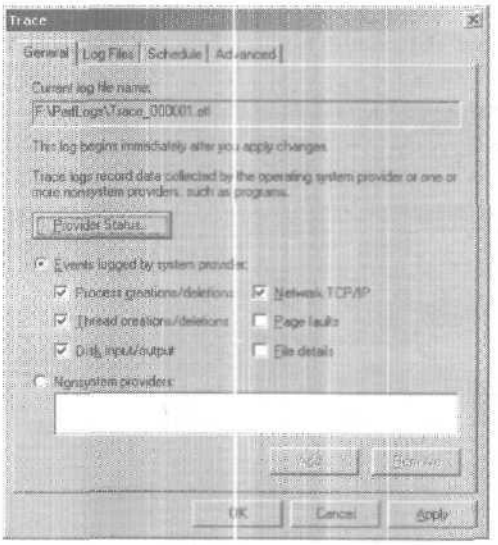


Рис. 3-16. Выберите на вкладке General поставщика, используемого при трассировке.

3. Чтобы отследить события ОС, нажмите кнопку параметра Events Logged By System Provider. Теперь можно выбирать события системы для отслеживания.

Внимание! Регистрация сбоев страниц и событий файлов сильно нагружает сервер и вызывает быстрый рост файлов журнала. Поэтому собирайте эти сведения только в течение ограниченного времени.

4. Если вы хотите отследить другого поставщика, нажмите кнопку параметра Nonsystem Providers (Несистемные поставщики) и щелкните Add. Появится диалоговое окно Add Nonsystem Providers, где можно выбрать отслеживаемых поставщиков.

5. Выбрав отслеживаемых поставщиков и события, щелкните вкладку Log Files. Теперь можно конфигурировать файл трассировки, как описано в п. 6 раздела «Создание журналов счетчиков». Единственное отличие: здесь другие типы файлов журнала:
   - Sequential **Trace** File (Файл последовательной трассировки) последовательно записывает события в журнал трассировки до максимального размера файла (если задан);
   - **Circular Trace File** (Файл циклической трассировки) заменяет старые данные новыми, когда файл достигает заданного предела.
6. Выберите вкладку Schedule, затем задайте время запуска и остановки трассировки.
7. Можно задать запуск журнала вручную или автоматически в определенный день. Выберите нужный параметр, затем задайте день запуска.
8. Можно задать остановку журнала вручную, по истечении определенного периода времени (например, семи дней), в определенный день и время или когда файл журнала наполнится (если вы задали определенный предел размера файла).
9. Завершив настройку расписания журнала, щелкните OK. Журнал будет создан, и им можно будет управлять, как описано в разделе «Создание и управление журналом производительности».

Воспроизведение журналов производительности

При устранении проблем часто требуется записывать данные о производительности на протяжении длительного периода времени, а потом анализировать эти данные.

1. Настройте автоматическую запись в журнал, как описано в разделе «Журналы производительности».
2. Загрузите файл журнала в Performance Monitor, когда будете готовы анализировать данные. Для этого щелкните кнопку View Log File Data в панели инструментов Performance Monitor. Появится диалоговое окно Select Log File.
3. В списке Look In откройте каталог журнала, затем выберите журнал для просмотра. Щелкните Open (Открыть).

4. Зарегистрированные счетчики доступны для отображения. Щелкните кнопку Add (Добавить) в панели инструментов, затем выберите счетчики для отображения.

Конфигурация сигналов оповещения для счетчиков производительности

Сигналы оповещения позволяют получать уведомления в ответ на определенные события или когда достигаются определенные пороги производительности. Эти оповещения можно отправлять как сетевые сообщения или записывать в журнал событий приложения. Оповещения могут запускать приложения и журналы производительности.

Чтобы добавить оповещения в Performance Monitor, сделайте так.

1. Выбрав Alerts в правой панели консоли Performance, щелкните правой кнопкой правую панель. В контекстном меню выберите New Alert Settings (Новые параметры оповещений).

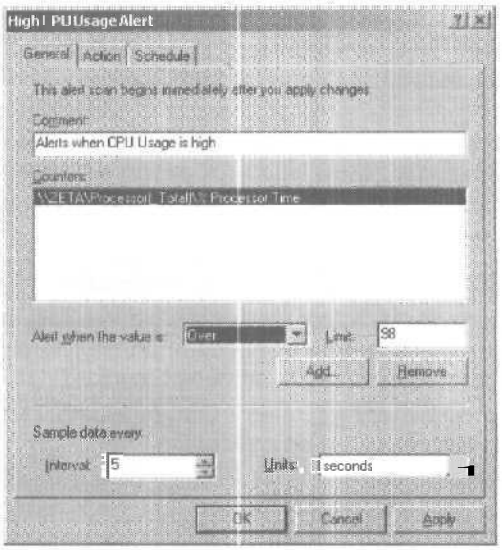


Рис. 3-17. Конфигурация счетчиков, запускающих оповещения.

2. В диалоговом окне New Alert Settings наберите имя сигнала оповещения, например Processor Alert или Disk I/O Alert. Щелкните OK. Откроется окно (рис. 3-17).
3. На вкладке General введите дополнительное описание оповещения. Затем щелкните Add,чтобы открыть окно Select Counters To Log. Это окно похоже на окно Add Counters (рис. 3-12).
4. В окне Select Counters To Log добавьте счетчики, запускающие оповещение, и щелкните Close.
5. В панели Counters выберите первый счетчик, затем в поле Alert When The Value Is... (Оповещать, когда значение) задайте условие, при котором запускается оповещение для этого счетчика. Оповещения могут запускаться, когда значение счетчика будет выше или ниже установленного. Выберите Over или Under и установите значение триггера. Единицы измерения — любые, подходящие для выбранного счетчика (счетчиков). Например, для оповещения при загруженности процессора более, чем на 98%, щелкните Over, а затем наберите 98. Повторите эту процедуру для других выбранных счетчиков.
6. В поле Sample Data Every... (Сжимать показания каждые) введите интервал сжатия и выберите формат времени в секундах, минутах, часах или днях. Интервал сжатия определяет, когда собираются новые данные. Например, при сжатии каждые 10 минут журнал обновляется каждые 10 минут.

Внимание! Не проводите сжатие слишком часто. Это отнимает системные ресурсы и может помешать серверу вовремя отвечать на запросы пользователей.

7. Выберите вкладку Action (рис. 3-18). Теперь можно определить действия, происходящие при запуске оповещения:
   - **Log An Entry In The Application Event Log** создает записи в журнале для оповещений;
   - **Send A Network Message To** отправляет сетевое сообщение на определенный компьютер;
   - **Run This Program** задает полный путь файла программы или сценария, выполняемого при срабатывании оповещения;

- Start **Performance Data Log** задает запуск журнала счетчика при срабатывании оповещения.

Совет Можно выполнить любой тип исполняемого файла, включая командные сценарии с расширением .BAT или .CMD и сценарии Windows с расширением .VB, .JS, PL или .WSC. Чтобы передать аргументы в сценарий или приложение, используйте ганель Command Line Arguments. Обычно аргументы переда·отся как отдельные строки. Однако при выборе Single Argument String аргументы передаются в списке с разделением запятыми в отдельной строке. Список Example Command Line Arguments в нижней части вкладки показывает, как должны передаваться аргументы.

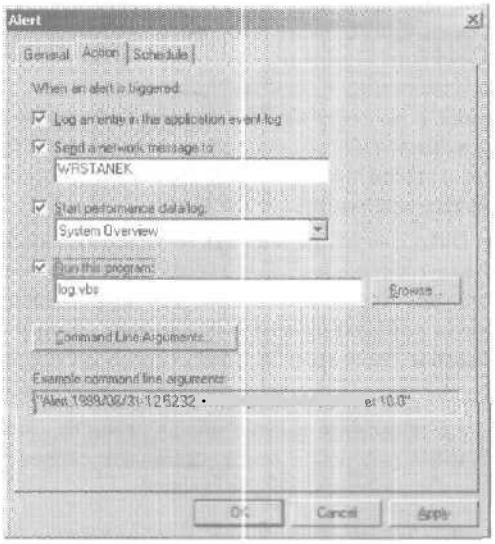


Рис. 3-18. Задайте действия, исполняемые при срабатывании оповещения.

8. Выберите вкладку Schedule (Расписание), затем определите запуск и остановку оповещения. Например, можно настроить запуск оповещений в пятницу вечером и их остановку в понедельник утром. Каждый раз при срабатывании оповещения в этот период исполняется определенное действие (действия).

9. Можно настроить запуск оповещений вручную или автоматически в определенный день. Выберите нужный параметр и определите дату запуска.
10. Можно настроить остановку оповещений вручную по истечении определенного срока, например, 7 дней или в определенный день и время.
11. Настроив расписание оповещений, щелкните OK. Оповещение будет создано, и им можно будет управлять аналогично тому, как управляют журналами счетчиков и трассировки.

Глава 4

Автоматизация административных задач, политики и процедур

Выполнение рутинных задач день за днем, настройка системной политики и объяснение пользователям азов работы с ОС – нерациональная трата времени. Ваша работа была бы гораздо эффективнее, если б вы могли автоматизировать эти задачи и сосредоточиться на более важных делах. Повышение производительности и возможность меньше заниматься мелочами в ущерб решению серьезных проблем — это и есть задача автоматизации.

В Microsoft Windows 2000 масса ресурсов, позволяющих автоматизировать административные задачи, политику и процедуры. В этой главе мы затронем:

- управление групповой политикой;
- управление сценариями пользователей и компьютеров;
- планирование выполнения задач.

Управление групповой политикой

Групповая политика упрощает администрирование, предоставляя администраторам централизованный контроль над привилегиями, разрешениями и возможностями пользователей и компьютеров. Групповая политика позволяет:

- создавать централизованно управляемые каталоги для особых папок, например Desktop (Рабочий стол), — см. ниже раздел «Централизованное управление особыми папками»;
- контролировать доступ к компонентам Windows, системным ресурсам, сетевым ресурсам, функциям панели управления, рабочему столу и меню Start (Пуск) — см. об

этом раздел «Использование административных шаблонов для настройки политики»;

- настроить сценарии пользователей и компьютеров для выполнения в заданное время — см. об этом раздел «Управление сценариями пользователя и компьютера»;
- конфигурировать политику для снятия блокировки с учетной записи, для паролей, аудита, присвоения пользовательских прав и безопасности — см. часть II этой книги.

Понятие групповой политики

Групповую политику можно рассматривать как набор правил управления пользователями и компьютерами. Групповую политику можно применять в нескольких доменах, в индивидуальных доменах, в подгруппах внутри домена или в индивидуальных системах. В индивидуальных системах применяется *локальная групповая политика* — она хранится только на локальной системе. Другие групповые политики связаны как объекты в службе Active Directory.

Чтобы понять, что такое групповая политика, нужно представлять структуру службы каталогов Active Directory. В Active Directory логические объединения доменов называются *сайтами,* а подгруппы внутри домена — *организационными подразделениями* (ОП). Так, в вашей сети могут быть сайты NewYorkMain, CaliforniaMain и WashingtonMain. Внутри сайта WashingtonMain могут быть домены SeattleEast, Seattle West, SeattleNorth и SeattleSouth. Внутри домена SeattleEast могут быть ОП Infirmation Services (IS), Engineering и Sales.

Групповая политика применяется только в системах с Windows 2000. Политика для систем на базе Windows **NT** 4.0 настраивается при помощи System Policy Editor (poledit.exe). Для Windows 95 и Windows 98 нужен System Policy Editor, поставляемый с этими ОС, затем следует копировать файл политики в общий ресурс SYSVOL на контроллере домена.

В каком порядке применяют несколько политик

Если политик несколько, они применяются в таком порядке:

1. Политики Windows NT 4.0 (NTConfig.pol).
2. Локальные групповые политики.
3. Групповые политики сайта.

4. Групповые политики домена.
5. Групповые политики ОП.
6. Групповые политики дочернего ОП.

Если параметры политик конфликтуют, то параметры политики, применявшиеся позже, обладают приоритетом и заменяют заданные ранее. Например, политика ОП обладает приоритетом над групповой политикой домена. У правила приоритета есть и исключения (см. раздел «Блокировка, перекрытие и отключение политики»).

Когда применяются групповые политики

Параметры политики делятся на две основные категории:

- применяемые к компьютерам;
- применяемые к пользователям:

Первые применяются обычно при загрузке системы, вторые — при входе в систему.

Точная последовательность событий часто важна при устранении неполадок в системе. Во время загрузки и регистрации происходят следующие события.

1. После запуска сети Windows 2000 применяет компьютерные политики. По умолчанию они применяются по очереди в указанном порядке. Интерфейс пользователя не отображается при обработке компьютерных политик.
2. Windows 2000 выполняет сценарии загрузки. По умолчанию они исполняются по очереди. Для выполнения очередного сценария нужно, чтобы выполнился предыдущий или прошло время его таймаута. Исполнение сценария не отображается для пользователя, если это не было задано.
3. Пользователь нажимает CTRL+ALT+DEL для входа в систему. Проверив его подлинность, Windows 2000 загружает профиль пользователя.
4. Windows 2000 применяет пользовательские политики. По умолчанию они применяются по очереди в указанном порядке. Интерфейс пользователя отображается при обработке политик пользователя.
5. Windows 2000 выполняет сценарии входа в систему. Сценарии входа в систему групповой политики исполняются одновременно по умолчанию. Исполнение сценария не

отображается для пользователя, если это не было задано. Сценарии в общем ресурсе Netlogon выполняются последними в окне обычной командной оболочки, как в Windows XT 4.0.

6. Windows 2000 отображает интерфейс стартовой оболочки, сконфигурированный в Group Policy.

Управление локальными групповыми политиками

У каждого компьютера с Windows 2000 есть одна локальная групповая политика. Локальной политикой на компьютере управляют так.

1. Откройте диалоговое окно Run (Запуск программы), щелкнув Start (Пуск), затем Run.
2. Наберите mmc в поле Open, затем щелкните OK. Откроется Microsoft Management Console (MMC).
3. В MMC щелкните Console (Консоль), затем Add/Remove Snap-In (Добавить/Удалить оснастку). Откроется диалоговое окно Add/Remove Snap-In.
4. На вкладке Standalone щелкните Add (Добавить).
5. В диалоговом окне Add Snap-In щелкните Group Policy (Групповая политика), затем Add. Откроется диалоговое окно Select Group Policy Object.
6. Щелкните Local Computer для изменения локальной политики на вашем компьютере или Browse — для поиска локальной политики на другом компьютере.
7. Щелкните Finish (Готово), затем Close (Закрыть).
8. Щелкните OK. Теперь можно управлять локальной политикой на выбранном компьютере. См. подробнее об этом раздел «Работа с групповыми политиками».

Локальные групповые политики на каждом компьютере с Windows 2000 хранятся в папке %SystemRoot%\system32\GroupPolicy. В ней содержатся следующие подпапки:

- **Adm** хранит файлы административных шаблонов, используемые в данный момент; файлы имеют расширение .adm; папка Adm находится только на контроллерах домена;
- **Machine** хранит сценарии компьютера в папке Script, а также регистрационную информацию о политике для HKEY_LOCAL_MACHINE (HKLM) в файле Rcgistry.pol;

- **User** хранит сценарии пользователей в папке Script и регистрационную информацию о политике для HKEY_CURRENT_USER (HKCU) - в файле Registry.pol.

Внимание! Не изменяйте эти папки и файлы напрямую — лучше используйте соответствующие свойства консоли Group Policy.

Управление политиками сайта, домена и ОП

У каждого сайта, домена и ОП может быть одна (или более) групповая политика. Групповые политики, перечисленные в списке Group Policy выше, обладают более высоким приоритетом, чем политики, приведенные ниже в списке. Как уже говорилось, групповые политики, настроенные на этом уровне, ассоциируются с Active Directory. Это гарантирует, что политики сайта правильно применяются в соответствующих доменах и ОП.

Создание и изменение политик сайта, домена и ОП

Политики сайта, домена и ОП можно создавать и изменять.

1. Оснастка Group Policy для сайтов запускается ил консоли Active Directory Sites And Services (Active Directory — сайты и службы).
2. Для доменов и ОП - из консоли Active Directory Users And Computers (Active Directory — пользователи и компьютеры).
3. В корне консоли щелкните правой кнопкой сайт, домен или ОП, в котором хотите создать или управлять групповой политикой, и выберите Properties (Свойства). Откроется диалоговое окно свойств.
4. Выберите вкладку Group Policy. Существующие политики перечислены в списке Group Policy Object Links (рис. 4-1).
5. Чтобы создать политику или изменить существующую, щелкните New (Создать). Теперь можно настроить политику (см. раздел «Работа с групповыми политиками»).
6. Чтобы изменить существующую политику, выберите ее и щелкните Edit (Изменить). Теперь ее можно изменять (см. раздел «Работа с групповыми политиками»).
7. Кнопки Up или Down позволяют изменить приоритет политики (т. е. ее положение в списке связей ОГП).

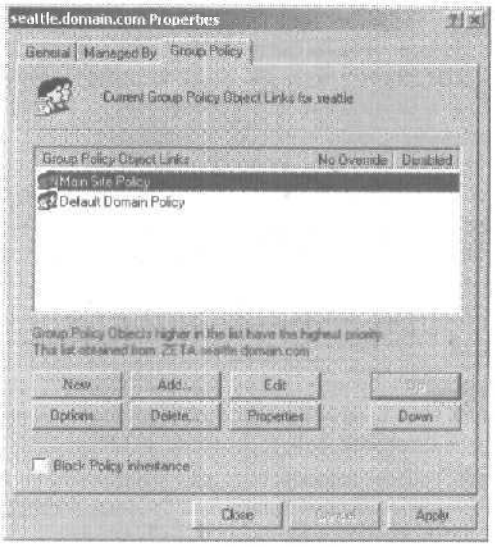


Рис. 4-1. Вкладка Group Policy служит для создания и изменения политик.

Групповые политики сайта, домена и ОП хранятся в папке %SystemRoot%\SYSVOL\domain\policies на контроллере домена. В этих индивидуальных папках политик вы найдете папки:

- Adm хранит файлы административных шаблонов с расширением .adm, *используемые* в данный момент; папка Adm есть только на контроллерах домена;
- **Machine** хранит сценарии компьютера в папке Script, а также реестровые политики для раздела HKEY_LOCAL_MACHINE (HKLM) в файле Registry.pol;
- **User** хранит сценарии пользователей в папке Script, а также реестровые политики для раздела HKEY_CURRENT_USER (HKCU) в файле Registry.pol.

Внимание! Не изменяйте эти папки и файлы напрямую — лучше используйте соответствующие свойства консоли Group Policy.

Блокировка, перекрытие и отключение политики

Наследование политики можно блокировать на уровне сайта, домена и ОП. Это значит, что вы можете либо блокировать, либо применять политики. На уровне сайта и домена также можно выполнять политику, или отказываться, или блокировать ее. Это позволяет администраторам высшего уровня выполнять политики и предотвращать их блокирование. Другой доступный параметр — отключение политики. Политику можно отключать частично или полностью, фактически не удаляя ее.

Эти параметры политики конфигурируются в следующей последовательности.

1. **Перейдите на вкладку Group** Policy для **работы** с нужным **сайтом,** доменом **или ОП,** как **описано в** разделе «Создание и изменение **политик** сайта, домена **и** ОП».
2. Выберите Block Policy Inheritance для предотвращения наследования политик более высокого уровня (если для этих политик не включен параметр No Override).
3. Параметр No Override (Не перекрывать) позволяет предотвратить блокирование политиками нижнего уровня параметров политики. Включите или выключите параметр No Override, дважды щелкнув в соответствующем столбце справа от элемента групповой политики. Галочка показывает, что параметр включен.
4. Параметр Disabled позволяет предотвратить применение политики. Настройте или очистите параметр Disabled, дважды щелкнув в соответствующем столбце справа от элемента групповой политики. Галочка показывает, что параметр включен.

Совет Отключить политику можно, заблокировав ветви параметров Computer Configuration или User Configuration, или и тех, и тех. Для этого щелкните Properties на вкладке Global Policy, затем пометьте или сбросьте флажок Disable Computer Configuration Settings (Отключить параметры конфигурации компьютера) и Disable User Configuration Settings (Отключить параметры конфигурации пользователя).

Применение существующей политики к новой области в сети

Любая созданная групповая политика может быть связана с другим компьютером, ОП, доменом или сайтом. Связывая

политику с другим объектом, можно использовать параметры политики без их воссоздания.

Вот как применить к новому месту в сети существующую политику.

1. Перейдите на вкладку Group Policy для нужных сайта, домена или ОП.
2. На вкладке Group Policy щелкните Add. Откроется диалоговое окно Add A Group Policy Object Link (Добавить ссылку на объект групповой политики) (рис. 4-2).

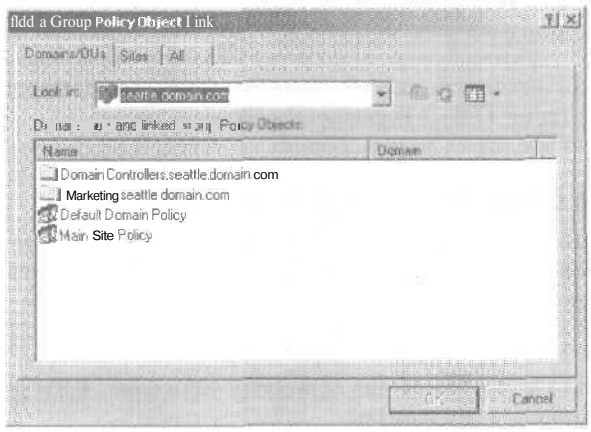


Рис. 4-2. Диалоговое окно Add A Group Policy Object Link позволяет связать существующие политики с новыми местами без воссоздания политики.

3. Используйте вкладки и поля, чтобы найти групповую политику, которую хотите применить для текущего размещения. Выбрав политику, щелкните OK.
4. Active Directory создает связь между объектом групповой политики (ОГП) и контейнером сайта- домена или ОП, с которым вы работаете. Модифицируя политику в любом месте, вы изменяете образец объекта, и изменения вступают в силу глобально.

Удаление групповой политики

Вы можете отключить или удалить те групповые политики, которые не используете.

1. Перейдите на вкладку Group Policy для работы с нужным сайтом, доменом или ОП (см. раздел «Создание и изменение политик сайта, домена и ОП»).
2. Выберите политику, которую хотите удалить, и щелкните Delete.
3. Если политика связана, можно удалить лишь связь, не затрагивая другие контейнеры, использующие эту политику. Для этого в диалоговом окне Delete выберите Remove The Link From The List (Изъять ссылку из списка, не удаляя объект).
4. Если политика связана, связь и соответствующий ОГП можно удалить, при этом политика удаляется окончательно. Для этого выберите Remove The Link And Delete The Group Policy Object Permanently (Изъять ссылку из списка и окончательно удалить объект групповой политики).

Работа с групповыми политиками

Выбрав политику для изменения или создав новую, вы будете использовать консоль Group Policy для работы с групповыми политиками.

Знакомство с консолью Group Policy

В консоли Group Policy два основных узла (рис. 4-3), которые позволяют настраивать:

- **Computer Configuration** — политики применяемые, к компьютерам независимо от того, кто регистрируется;
- **User Configuration** — политики, применяемые к пользователям, независимо от того, с какого компьютера они входят в сеть.

Точная конфигурация Computer Configuration и User Configuration зависит от настроенных дополнений и типа создаваемой политики. Обычно и у Computer Configuration, и у User Configuration имеются следующие подузлы.

- **Software** Settings (Конфигурация программ) настраивает политики для параметров и установки ПО; при настройке ПО подузлы могут добавляться в Software Settings;
- **Windows Settings** (Конфигурация Windows) настраивает политики для перенаправления папок, сценариев и безопасности;

- Administrative **Templates** (Административные шаблоны) настраивает политики для ОС, компонентов Windows и программ; административные шаблоны конфигурируются при помощи файлов шаблонов, которые можно добавлять/удалять.

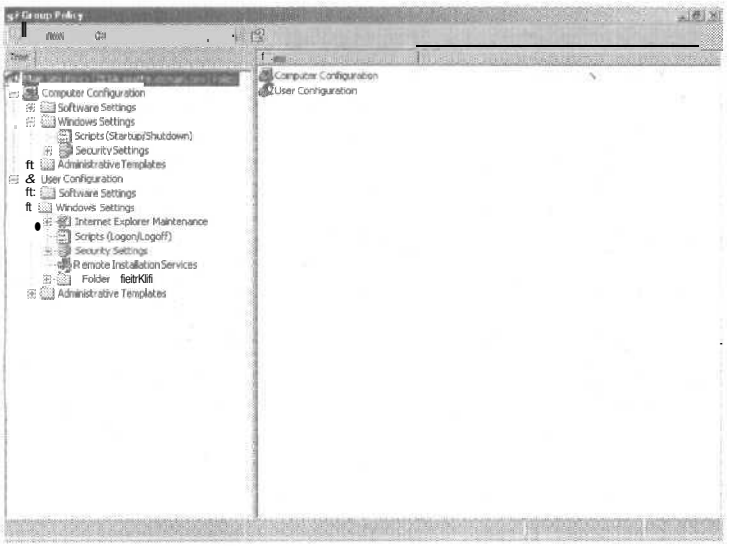


Рис. 4-3. Конфигурация консоли Group Policy зависит от типа создаваемой политики и установленных дополнений.

Примечание Полное обсуждение всех доступных параметров выходит за рамки этой книги. В дальнейших разделах мы сосредоточимся на перенаправлении папок и административных шаблонах. О сценариях см. раздел «Управление сценариями пользователя и компьютера», о безопасности — часть II этой книги.

Централизованное управление специальными папками

Можно централизованно управлять специальными папками Windows 2000, перенаправляя их в центральный сетевой каталог вместо использования стандартных каталогов на отдельных компьютерах. Специальные папки, которыми можно централизованно управлять:

- Application Data;
- Desktop (Рабочий стол);
- Start Menu (Меню Пуск);
- My Documents (Мои документы);
- My Pictures (Мои рисунки).

Вы можете перенаправить специальную папку в единый сетевой каталог для всех пользователей или назначить каталоги, исходя из участия пользователей в группах безопасности. В любом случае убедитесь, что нужный вам. сетевой каталог доступен общим сетевым ресурсом. Подробнее о совместном использовании данных в сети см. главу 13.

Перенаправление специальной папки в единый каталог

1. Откройте консоль Group Policy для работы с нужным сайтом, доменом или ОП, как описано в разделе «Создание и изменение политик сайта, домена и ОП».
2. В узле User Configuration раскройте узел Windows Settings и выберите Folder Redirection (Перенаправление папки).
3. Щелкнув правой кнопкой папку, с которой хотите работать, например Application Data, выберите Properties. Откроется окно свойств (рис. 4-4).
4. На вкладке Target (Размещение) в списке Setting (Политика) выберите Basic — Redirect Everyone's Folder To The Same Location (Перенаправлять папки всех пользователей в одно место).
5. Введите в поле Target Folder Location (Размещение конечной папки) путь к централизованной папке. В ней будут храниться все данные специальной папки. Задавайте путь к общей папке в формате UNC, например \\Zeta\UserData. Для поиска папки щелкните Browse (Обзор) в диалоговом окне Browse For Folder (Обзор папок).

Совет По умолчанию данные всех пользователей хранятся вместе. Чтобы пользовательские данные распределялись по подпапкам, добавьте в путь переменную %UserName%. Например, вместо явного пути \\Zeta\UserData введите \\Zeta\UserData\%UserName%.

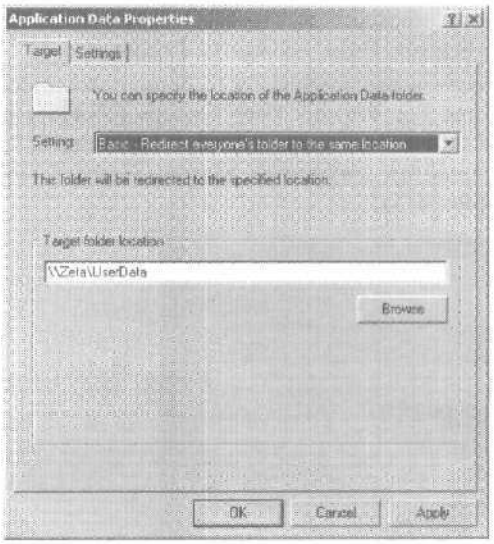


Рис. 4-4. Задайте параметры для перенаправления в диалоговом окне Application Data Properties.

6. Щелкните вкладку Settings и в следующих полях задайте дополнительные параметры:
   - Grant The User Exclusive Rights To ... (Предоставить исключительные права для ...) наделяет пользователей всеми правами доступа к их данным в специальной папке;
   - Move The Contents Of ... To The New Location (Перенести содержимое ... в новое место) перемещает данные в специальных папках с индивидуальных систем в центральную сетевую папку (папки).
7. Чтобы завершить процесс, щелкните OK,

Перенаправление специальной папки в зависимости от членства в группе

1. Откройте консоль Group Policy для работы с нужным сайтом, доменом или ОП.
2. В узле User Configuration вы найдете Windows Settings. Раскройте его двойным щелчком и выберите Folder Redirection.

3. Щелкнув правой кнопкой нужную специальную папку, например Application Data, выберите Properties.
4. На вкладке Target в списке Setting выберите Advanced — Specify Locations For Various User Groups (Указать различные места для разных групп пользователей). В диалоговое окно свойств добавится панель Security Group Membership (рис. 4-5).

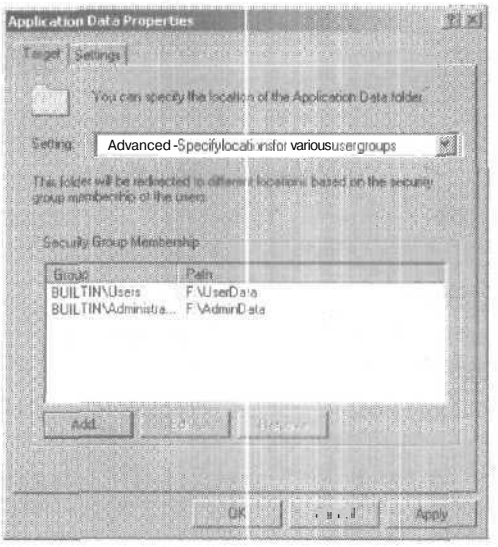


Рис. 4-5. Конфигурируйте дополнительное перенаправление в панели Security Group Membership.

5. Щелкните Add, чтобы открыть окно Specify Group And Location (Выбор группы и размещения). Или выберите существующий групповой элемент и щелкните Edit (Изменить) для изменения его параметров.
6. В поле Security Group Membership (Членство в группе безопасности) введите имя группы безопасности, для которой хотите включить перенаправление. Щелкните Browse, чтобы найти группу безопасности.
7. В поле Target Folder Location введите путь к общей папке. В ней будут храниться данные группы. Введите путь к общей папке в формате UNC, например \\Zeta\UserData. Для поиска папки щелкните Browse в диалоговом окне Browse For Folder.

Совет По умолчанию данные всех пользователей хранятся вместе. Чтобы пользовательские данные распределялись по подпапкам, добавьте в путь переменную %UserName%. Например, вместо явного пути \\2eta\UserData введите \\Zeta\UserData\%UserName%.

8. Щелкните OK. Затем повторите ни. 5-7 для других групп, которые хотите конфигурировать.
9. Добавив записи групп, щелкните вкладку Settings и в следующих полях задайте дополнительные параметры:
   - **Grant The User Exclusive Rights To ...** наделяет пользователей всеми правами доступа к их данным в специальной папке;
   - **Move The Contents Of ... To The** New **Location** перемещает данные в специальных папках с индивидуальных систем в центральную сетевую папку (папки).

Отмена перенаправления

Иногда требуется отменить перенаправление из конкретной специальной папки.

1. Откройте подузел Folder Redirection в консоли Group Policy.
2. Щелкнув правой кнопкой нужную специальную папку, выберите Properties.
3. Выберите вкладку Settings, затем убедитесь, что выбран соответствующий параметр Policy Removal. Доступны два параметра: Leave The Folder In The New Location When Policy Is Removed (После удаления политики переместить папку) или Redirect The Folder Back To The Local Userprofile Location When Policy Is Removed (После удаления политики перенаправить папку обратно в локальный профиль пользователя). При выборе первого файлы и папки остаются в перенаправленной папке, даже когда перенаправление удалено, при выборе второго файлы и папка возвращаются в локальную папку пользовательского профиля.
4. Выбрав параметр Policy Removal, щелкните Apply (Применить), затем — вкладку Target.
5. Чтобы удалить все определения перенаправления для специальной папки. в списке Setting выберите No Administrative Policy Specified.

6. Чтобы удалить перенаправления конкретной группы безопасности, выберите группу безопасности в панели Security Group Membership и щелкните Remove (Удалить).
7. Щелкните OK.

Настройка политик с помощью административных шаблонов

Административные шаблоны облегчают доступ к реестровым параметрам политики, которые может понадобиться конфигурировать.

Обзор административных шаблонов и политик

Набор административных шаблонов по умолчанию конфигурируется для пользователей и компьютеров в консоли Group Policy (рис. 4-6). Административные шаблоны можно добавлять/удалять. Любые изменения в политиках, совершаемые через административные шаблоны, сохраняются в реестре. Конфигурации компьютеров сохраняются в разделе HKEY_LOCAL_MACHINE (HKLM), а конфигурации пользователей - в HKEY_CURRENT_USER (HKCU).

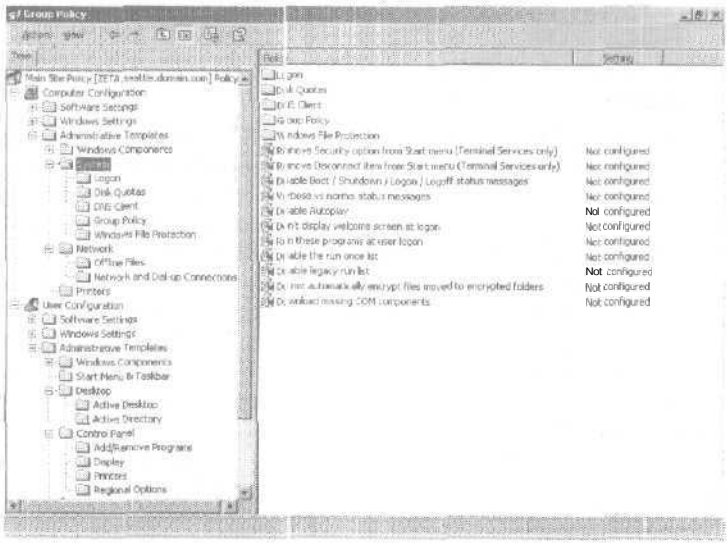


Рис. 4-6. Политики настраиваются при помощи административных шаблонов.

Настроенные шаблоны позволяет просмотреть узел Administrative Templates (Административные шаблоны) консоли Group Policy. Он содержит политики, конфигурируемые для локальных систем, ОП, доменов и сайтов. В ветвях Computer Configuration и User Configuration находятся разные наборы шаблонов. Можно вручную добавлять дополнительные шаблоны, содержащие новые политики, в консоль Group Policy, а также при настройке новых компонентов Windows.

Пользовательский интерфейс для узла Administrative Templates настраивается в файлах с расширением .adm. Эти текстовые файлы в формате ASCII можно редактировать или создавать в стандартном текстовом редакторе. При конфигурации политик в узле Administrative Templates параметры политики сохраняются в файлах Registry.pol. Для разделов реестра HKEY_LOCAL_MACHINE (HKLM) и HKEY_CURRENT_USER (HKCU) применяются отдельные файлы Registry.pol.

Узнать, какие политики административных шаблонов доступны, можно, просмотрев узлы Administrative Templates в консоли Group Policy. Вы увидите, что политики находятся в одном из трех состояний:

- Not Configured — политика не используется, и ее параметры не сохранены в реестре;
- Enabled — политика активно выполняется, и ее параметры сохраняются к реестре;
- Disabled — политика отключена и не выполняется, если не замещена; этот параметр сохраняется в реестре.

Включение, отключение и конфигурация политик

1. Откройте консоль Group Policy для работы с нужным сайтом, доменом или ОП.
2. Откройте папку Administrative Templates в узле Computer Configuration или User Configuration в зависимости от конфигурируемого типа политики.
3. В левой панели щелкните подпапку, содержащую нужные вам политики. Соответствующие политики отобразятся в правой панели.
4. Щелкните дважды или правой кнопкой политику и выберите Properties, чтобы открыть окно ее свойств.

5. Щелкните вкладку Explain для просмотра описания политики. Описание доступно, только когда определено в соответствующем файле с расширением .adm.
6. Для конфигурации состояния политики щелкните вкладку Policy, а затем используйте переключатели для изменения состояния политики:
   - **Not Configured** (Не задана);
   - **Enabled** (Включена);
   - **Disabled** (Отключена).

Примечание Компьютерные политики обладают приоритетом в Windows 2000. При конфликте между параметром компьютерной и пользовательской политики применяется компьютерная политика.

7. Включив политику, настройте любые дополнительные параметры на вкладке Policy (Политика), затем щелкните Apply (Применить).
8. Кнопки Previous Policy и Next Policy позволяют перейти к другим политикам в текущей папке. Конфигурируйте их тем же образом.
9. Настроив политики, щелкните OK.

Добавление или удаление шаблонов

Папки шаблонов в консоли Group Policy можно добавлять/удалять.

1. Откройте консоль Group Policy для работы с нужным сайтом, доменом или ОП.
2. Щелкните правой кнопкой папку Administrative Templates в узле Computer Configuration или User Configuration — для того тина шаблона, который вы хотите добавить/удалить. Откроется окно Add/Remove Templates (рис. 4-7).
3. Чтобы добавить новый шаблон, щелкните Add. В окне Policy Templates щелкните добавляемый шаблон, а затем — Open.
4. Для удаления существующего шаблона выберите шаблон для удаления и щелкните Remove.
5. Завершив добавление/удаление шаблонов, щелкните Close.

Управление сценариями пользователей и компьютеров

В Windows 2000 можно конфигурировать четыре типа сценариев;

- **Computer Startup** — выполняется во время загрузки;
- **Computer Shutdown** — выполняется перед завершением работы;
- **User Logon** — выполняется при входе пользователя в систему;
- User **Logoff** — выполняется при выходе пользователя из системы.

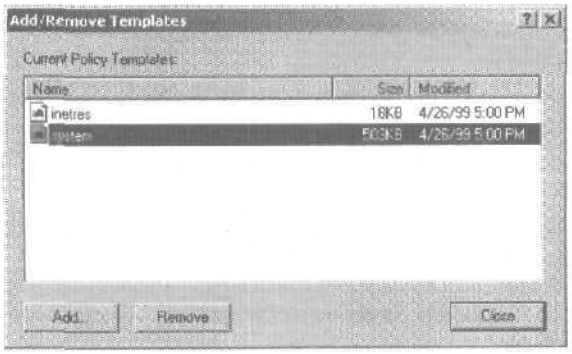


Рис. 4-7. Диалоговое окно Add/Remove Templates позволяет добавить шаблоны или удалить существующие.

Можно писать пакетные сценарии командного процессора с расширением .BAT или .CMD, или же сценарии для Windows Script Host (WSH). WSH — новый компонент Windows 2000 — позволяет использовать язык сценариев, например VBSscript, без встраивания его кода в Web-страницу. Для обеспечения универсальной среды исполнения WSH опирается на ядра сценариев — компоненты, определяющие базовый синтаксис и структуру отдельного языка сценариев. Windows 2000 оснащена ядрами сценариев VBScript и JScript. Доступны и другие ядра сценариев.

Назначение сценариев загрузки компьютера и завершения работы

Сценарии загрузки компьютера и завершения работы назначаются как часть групповой политики. Таким образом, все компьютеры — члены сайта, домена и/или ОП — автоматически исполняют сценарии при загрузке или завершении работы.

Примечание Сценарии загрузки компьютера можно назначить в виде назначенных заданий с помощью мастера Task Scheduler (см. раздел «Назначение заданий»).

Сценарий загрузки компьютера или завершения работы назначается так.

1. Для облегчения управления скопируйте нужные сценарии в папку соответствующей политики Computer\Scripts\Startup или Computer\Scripts\Shutdown. Политики хранятся в папке %SystemRoot%\SYSVOL\domain\policies на контроллерах домена.
2. Откройте консоль Group Policy для работы с нужным сайтом, доменом или ОП.
3. В узле Computer Configuration дважды щелкните папку Windows Settings. Затем щелкните Scripts.
4. Для работы со сценариями загрузки щелкните правой кнопкой Startup, затем выберите Properties. Или щелкните правой кнопкой Shutdown и выберите Properties для работы со сценариями Shutdown. Откроется диалоговое окно (рис. 4-8).

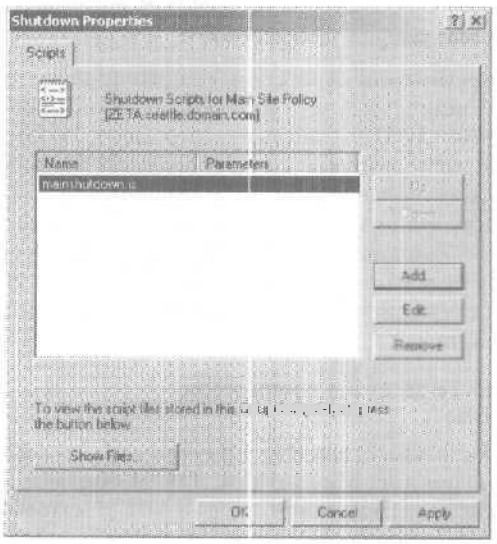


Рис. 4-8. Добавление, изменение и удаление сценариев компьютера в окне Shutdown Properties.

5. Щелкните Show Files. Если вы скопировали сценарий компьютера в нужное место в папке политик, вы должны увидеть этот сценарий.
6. Чтобы назначить сценарий, щелкните Add. Откроется окно Add A Script. В поле Script Name введите имя сценария, скопированного в папку соответствующей политики - Computer\Scripts\Startup или Computer\Scripts\Shutdown. В поле Script Parameter введите для WSH-сценария аргументы командной строки, которые нужно передать в сценарий, или параметры, которые нужно передать серверу сценариев. Повторите этот шаг для добавления других сценариев.
7. При загрузке или завершении работы сценарии исполняются в том порядке перечисления в окне свойств. Кнопки Up или Down позволяют упорядочить сценарии.
8. Если вы хотите позже изменить имя сценария или параметры, выберите сценарий в списке Script For и щелкните Edit.
9. Чтобы удалить сценарий, выберите его в списке Script For и щелкните Remove.

Назначение сценариев входа и выхода пользователя

Сценарии пользователей можно назначить одним из трех способов.

- Сценарии входа и выхода можно назначать как часть групповой политики. Таким образом, все пользователи — члены сайта, домена и/или ОП — автоматически исполняют сценарии при входе или выходе.
- Можно индивидуально назначать сценарии входа в консоли Active Directory Users And Computers. Таким образом, каждому пользователю или группе можно приписать отдельный сценарий входа (см. главу 9).
- Можно активизировать индивидуальные сценарии входа через механизм назначения заданий из мастера Task Scheduler (см. раздел «Назначение заданий»).

Пользовательский сценарий групповой политики назначается так.

1. Для облегчения управления скопируйте нужные вам сценарии в папку соответствующей политики User\Scripts\Lo-

gon или User\Scripts\Logoff. Политики хранятся в папке %SystemRoot%\SYSVOL\domain\policies на контроллерах домена.

2. Откройте консоль Group Policy для работы с нужным сайтом, доменом или ОП.
3. В узле User Configuration дважды щелкните папку Windows Settings, а затем — Scripts.
4. Для работы со сценариями входа щелкните правой кнопкой Logon, затем выберите Properties. Или щелкните правой кнопкой Logoff и выберите Properties. Откроется такое диалоговое окно (рис. 4-9):

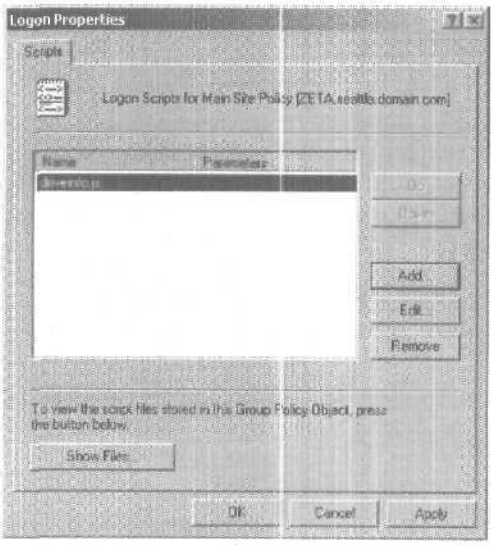


Рис. 4-9. Для добавления, изменения и удаления сценариев пользователя служит диалоговое окно Logon Properties.

5. Щелкните Show Files. Если вы скопировали сценарий пользователя в нужное место в папке политик, вы его увидите.
6. Щелкните Add для назначения сценария. Откроется окно Add A Script. В поле Script Name введите имя сценария, скопированного в панку соответствующей политики User\Scripts\Logon или User\Scripts\Logoff. В поле Script Parameter введите для WSH-сценария аргументы, которые

нужно передать в сценарий командной строки, или параметры, которые нужно передать серверу сценариев. Повторите этот шаг для добавления других сценариев.

7. При входе/выходе сценарии выполняются в порядке перечисления в окне свойств. Кнопки Up или Down позволяют упорядочить сценарии.
8. Если вы хотите позже изменить имя сценария или параметров, выберите сценарий в списке Script For и щелкните Edit.
9. Чтобы удалить сценарий, выберите его в списке Script For и щелкните Remove.

Назначение заданий

Администратору часто приходится выполнять обновление или профилактические работы в, так сказать, «личное» время. Но кому охота приходить на работу в 3 часа ночи в понедельник? Служба Task Scheduler позволяет назначить выполнение задания один раз или же его автоматическое выполнение в любое время дня или ночи.

Задания автоматизируются с помощью сценариев командных процессоров, сценариев Windows Script Host или приложений, исполняющих для вас нужные команды. Например, если вы хотите создавать резервные копии системного диска по будням в полночь, создайте сценарий, выполняющий резервные копии и записывающий результаты в файл журнала.

Средства назначения заданий

Назначать задания на локальных или удаленных системах в Windows 2000 помогают мастер Task Scheduler или AT-планировщик командной строки. У каждого способа есть свои преимущества и недостатки.

Мастер предоставляет удобный графический интерфейс. Это упрощает конфигурацию заданий, не заставляя думать о синтаксисе. Однако в этом случае у вас нет центрального места для проверки назначенных заданий во всей сети, и вам приходится вызывать мастер на каждой системе, которую надо конфигурировать.

С другой стороны, команда AT не имеет дружественного интерфейса: вам придется изучить синтаксис и вводить команды. Преимущество AT в том, что вы можете назначить от-

дельный сервер планировщиком заданий, просматривать и назначать задачи по всей сети с этого сервера.

Подготовка к назначению заданий

Task Scheduler по умолчанию регистрируется под учетной записью Local System. Обычно эта учетная запись не позволяет выполнять административные задачи. Поэтому настройте Task Scheduler для запуска под учетной записью, полномочной для выполнения заданий, которые вы хотите назначить. Вы также должны убедиться, что Task Scheduler готова к автоматическому запуску на всех системах, на которых вы назначаете задания. Настройте учетную запись запуска и регистрации Task Scheduler, как описано в главе 3.

Сценарий должен конфигурировать любые параметры пользователя. Это гарантирует, что все, что делает сценарий, находится под его контролем и что доменные пользовательские параметры, например проекции дисков, будут доступны.

Назначение заданий при помощи Task Scheduler

Task Scheduler позволяет назначать задачи на локальной или удаленной системе, с которой в данный момент установлено соединение. Вызвать Task Scheduler и просмотреть текущие назначенные задания можно из папки Scheduled Tasks (Назначенные задания).

Открытие папки **Scheduled Tasks**

Вы можете открыть папку Scheduled Tasks на локальной системе одним из следующих способов:

- запустите Проводник, дважды щелкните Control Panel (Панель управления), а затем — Scheduled Tasks (Назначенные задания);
- раскройте меню Start\Settings\Control Panel (Пуск\Настройка\Панель управления) и дважды щелкните Scheduled Tasks.

На удаленной системе папка Scheduled Tasks открывается так.

1. Запустите Explorer и и узле My Network Places найдите нужный компьютер.
2. Дважды щелкните значок компьютера, а затем — Scheduled Tasks.

Обзор и управление существующими заданиями

Записи в папке Scheduled Tasks показывают текущие назначенные задания (рис. 4-10).

1. Дважды щелкнув Add Scheduled Tasks (Добавить задание), запустите мастер Task Scheduler.
2. Дважды щелкните ярлык существующего задания для просмотра или изменения его свойств. Вы можете настроить дополнительные параметры на вкладке Settings.
3. Щелкните ярлык задания и нажмите Delete для удаления задания.

Рис. 4-10. Существующие задания перечислены в папке Scheduled Tasks. Щелкните Add Scheduled Task для запуска мастера.

Создание заданий при помощи мастера Task Scheduler

1. Запустите Task Scheduler, дважды щелкнув Add Scheduled Task в папке Scheduled Tasks, затем щелкните Next.
2. В диалоговом окне (рис. 4-11) выберите программу для назначения. Здесь перечислены основные приложения, зарегистрированные в системе, например Disk Cleanup и Synchronize. Здесь не показаны доступные сценарии.

Щелкните Browse, чтобы открыть окно Select Program To Schedule (Выберите приложение, для которого следует составить расписание), и найдите командный процессор или сценарий WSH, выполнение которого хотите запланировать.

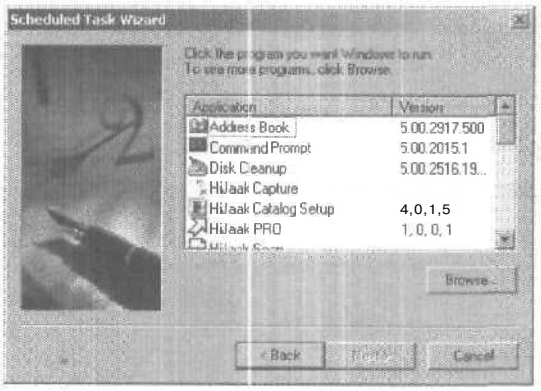


Рис. 4-11. Выберите программу для выполнения. Щелкните Browse для поиска сценариев и других приложений.

3. Введите имя задания (рис. 4-12). Имя должно быть коротким, но описательным, чтобы вы могли сразу вспомнить, что выполняет задание.

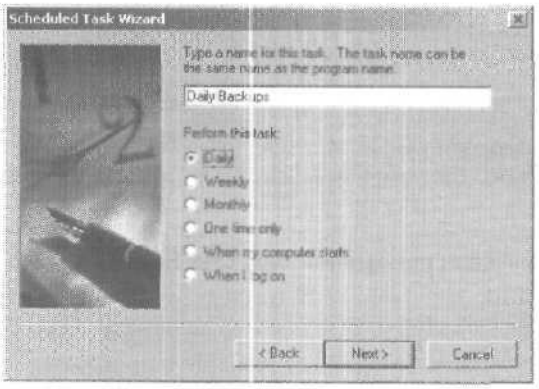


Рис. 4-12. Введите имя задания и настройте расписание его выполнения.

4. Выберите расписание выполнения задания. Задания можно назначать периодически (ежедневно, еженедельно или ежемесячно) или когда происходит конкретное событие, например, при запуске компьютера или входе пользователя.
5. Щелкните Next и выберите день и время выполнения назначенного задания. Появление следующего диалогового окна зависит от того, когда назначено выполнение задания.
6. Если вы настроили ежедневное выполнение задания, появится диалоговое окно для выбора дня и времени (рис. 4-13). Можно конфигурировать ежедневное выполнение так:
   - **Every Day** — 7 дней в неделю;
   - **Weekdays** — с понедельника по пятницу;
   - **Every...Days** — каждые 2, 3,...N дней.

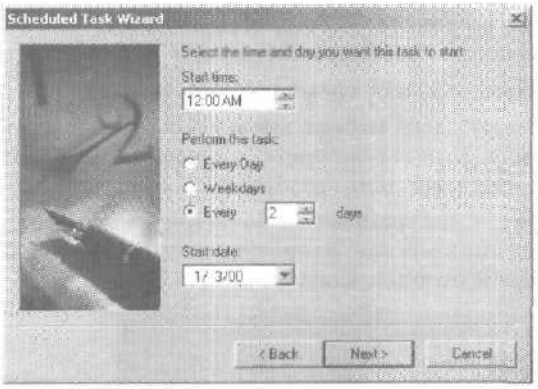


Рис. 4-13. Настройка ежедневного выполнения задания.

7. Если вы выбрали еженедельное выполнение задания, появится диалоговое окно выбора дня и времени (рис. 4-14). Сконфигурируйте задание в следующих полях:
   - **Start Time** — настраивает время запуска задания;
   - **Every...Weeks** — позволяет выполнять задание каждую неделю, каждые две недели или каждые N недель.
   - **Select The Day(s) Of The Week Below** — настраивает день (дни) недели, когда выполняется задание, например, понедельник или понедельник и пятница.

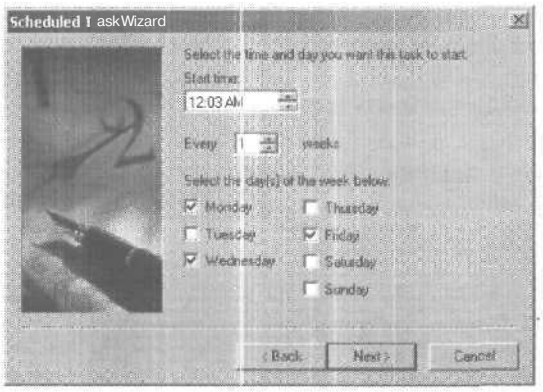


Рис. 4-14. Конфигурация еженедельно назначаемого задания.

8. Если вы выбрали ежемесячное выполнение задания, появится окно выбора дня и времени (рис. 4-15). Конфигурируйте задание, используя следующие поля:

- Start Time — задает время запуска задания;
- Day — задает день месяца, когда выполняется задание. Например, если вы выберете 5, задание будет выполняться на пятый день месяца;
- **The...Day** — настраивает выполнение заданий на n-й день недели в месяце, например, второй понедельник или третий вторник каждого месяца;

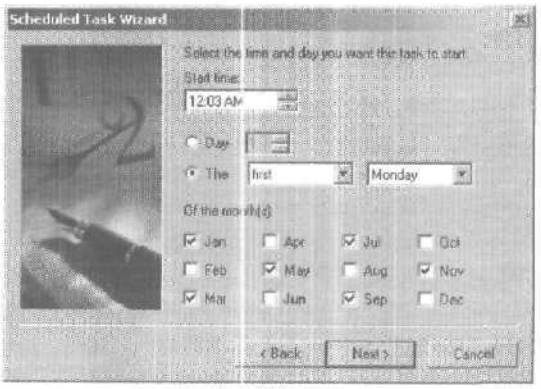


Рис. 4-15. Конфигурация ежемесячно назначаемого задания.

- **Of The Month(s)** — флажки задают, по каким месяцам выполняется задание.

9. **Если вы выбрали One Time Only,** появится **окно** выбора дня **и времени** (рис. **4-16).** Настройте **время и лень** запуска.

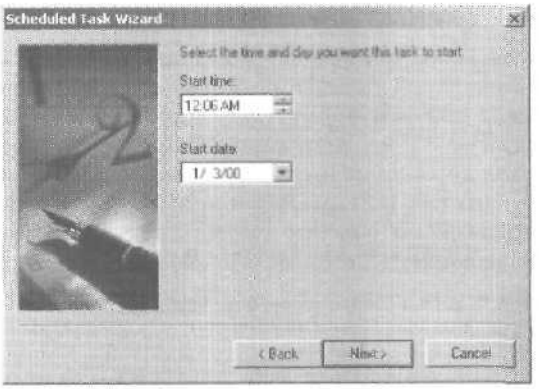


Рис. 4-16. Конфигурация однократного задания.

10. В заданиях, выполняемых при загрузке компьютера или при входе пользователя, не надо устанавливать день и время. Задание выполняется автоматически, когда происходит событие загрузки или входа.

Совет Чтобы настроить задание, выполняемое при загрузке для конкретного пользователя, войдите под его учетной записью и запустите мастер.

11. Задав день и время запуска, щелкните Next. Затем введите имя пользователя и пароль, которые могут применяться при выполнении назначенного задания. У этого имени пользователя должны быть соответствующие разрешения и привилегии для выполнения назначенного задания.
12. Последнее диалоговое окно мастера содержит сводку назначения задания. Щелкните Finish (Готово) для завершения процесса назначения. Если произойдет ошибка, появится сообщение. Щелкните OK. Задание должно быть создано. После этого дважды щелкните в Проводнике задание, чтобы исправить проблемы в окне свойств.

Назначение заданий при помощи команды AT

Контролировать службы Task Scheduler позволяет и команда AT: вы можете назначать задания повсюду в сети, не входя на удаленные системы. Можно настраивать выполнение заданий однократно или периодически по расписанию.

Использование команды AT

Для назначения задач при помощи команды AT вы должны быть членом локальной группы администраторов. Задания назначаются в 24-часовом формате, где 12:00 — это полдень, а 00:00 — полночь. AT не загружает автоматически интерпретатор команд до выполнения встроенных утилит командной строки, таких как DEL, COPY или MOVE. Потребуется явная загрузка cmd.exe в начале команды. Например, чтобы скопировать *c:\mydata*.** в *e:\backups\mydata*, введите:

```
AT 00:00/every:M,T,W,Th,F"cmd/c copy/Q c:\mydata\*.*
e:\backups\mydata"
```

Работая с программами и утилитами, у которых есть отдельные исполняемые файлы, не запускайте отдельный экземпляр интерпретатора команд. Вы можете работать прямо с исполняемым файлом. Исполняемый файл должен быть в каталоге, доступном через переменную окружения %PATH%. Вот как можно назначать сценарий создания резервных копий, выполняемый через день в 1:00:

```
AT 01:00/every:1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31
backup.js
```

При использовании дней, обозначенных цифрами, у вас может быть любое значение от 1 до 31. Выполнение заданий также назначается *в* соответствии с текущим днем. Для этого определите только время запуска, а не день выполнения. Так, запустить сценарий очистки в 3:00 позволяет команда:

```
AT 03:00 cleanup.js
```

Можно назначать выполнение заданий на другой день. Так, если сегодня вторник и вы хотите, чтобы задание было выполнено в пятницу, можете дать команду:

```
AT 08:10/nextF update.vbs
```

Обычно задания выполняются как фоновые процессы. Однако можно настроить интерактивное выполнение заданий. Для этого служит ключ */interactive,* например:

```
AT 03:00/interactive/every:T,Th backup.vbs
```

Назначение заданий на удаленных системах

Команда AT упрощает назначение задач, выполняемых на удаленных системах. Введите UNC-имя компьютера до настройки других параметров. Например, если вы хотите назначить выполнение задания на компьютере с именем PLUTO, введите в командной строке на вашей системе:

```
AT\\PLUTO 08:10/next:F update.vbs
```

Вы также можете указать IP-адрес *компьютера:*

```
AT\\192.51.62.8 09:30/every:M,W,F cleanup.js
```

Используйте этот параметр, только если IP-адрес статичен.

Назначение задач на удаленных системах предполагает, что:

- вы настроили службу Task Scheduler на PLUTO для использования входа с соответствующими разрешениями;
- служба Task Scheduler выполняется;
- сценарии расположены в каталогах, которые можно найти в пути, настроенном для учетной записи входа службы.

Обзор назначенных заданий

Можно просматривать назначенные задания на локальных и удаленных системах. На локальной системе введите AT в командной строке и нажмите Enter. На удаленной системе введите **AT** перед UNC-именем нужной нам системы:

AT\\ PLUTO

При просмотре заданий вы получаете следующий результат:

```
Status  ID   Day       Time      Command Line
        1    EachMWF   3:00 AM   backup.vbs
        2    EachTTh   5:00 AM   cleanup.js
        3    EachSu    8:00 AM   update.js
```

- **Status** - указывает статус каждого задания. Элемент «пусто» свидетельствует о статусе OK. Иначе будет выдано сообщение об ошибке, например ERROR.

- Ш — показывает уникальный идентификатор для каждого задания.
- Day — показывает, когда назначено выполнениезадания. Повторные задания начинаются с ключевого слова Each, например Each M - каждый понедельник. Однократно выполняемые задания начинаются с ключевого слова Next, например Next 3, т. с. в следующий раз это будет третий день месяца.
- **Time** — показывает время, на которое назначено выполнение программы. Заметьте, что время для назначения заданий отображается в 12-часовом формате.
- **Command Line** — показывает команду или исполняемый файл, выполняемый в назначенное время.

Для отображения индивидуальных заданий можно использовать код задания:

```
AT 2
```

или:

```
AT\\zeta 2
```

Удаление заданий

Также можно использовать код задания для удаления заданий или для отмены всех назначенных заданий. Отдельное задание удаляется так:

```
AT 2/delete
```

или:

```
AA\zeta  2/delete
```

Все задания отменяются вводом ключа */delete* без кода:

```
AT/delete
```

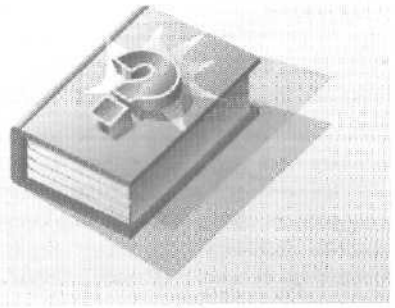
или:

```
AT\\zeta/delete
```

Часть II

Администрирование служб каталогов Microsoft Windows 2000

В этой части описаны задачи управления службами каталогов Microsoft Windows 2000. В главе 5 вы познакомитесь со службой каталогов Active Directory. В главе 6 изучаются основные задачи администрирования Active Directory. В главе 7 дано понятие системных учетных записей, встроенных групп, прав пользователей, встроенных возможностей и неявных групп. О создании учетных записей пользователей и групп рассказано в главе 8. Методика управления существующими учетными записями пользователей и групп разъясняется в главе 9.



Глава 5

Использование службы Active Directory

Расширяемая и масштабируемая служба каталогов Active Directory, позволяет эффективно управлять сетевыми ресурсами.

Знакомство со службой Active Directory

Active Directory — сердце Microsoft Windows 2000. Все административные задачи отражаются в Active Directory. Технология Active Directory основана на стандартных Интернет-протоколах, и се конструкция помогает четко определять структуру сети.

Active Directory и DNS

Active Directory использует доменную систему имен (Domain Name System, DNS). DNS — стандартная служба Интернета, которая организует группы компьютеров в домены. В отличие от линейной структуры доменов Windows NT 4.0 домены DNS имеют иерархическую структуру. Иерархия доменов DNS образует основу Интернета, и разные уровни в этой иерархии идентифицируют компьютеры, домены организаций и домены верхнего уровня. DNS также служит для преобразования имен узлов, например microsoft.com, в числовые адреса TCP/IP, например 192.168.19.2. Средствами DNS иерархия доменов Active Directory может быть вписана в пространство Интернета или может быть отдельной и закрытой.

Для доступа к ресурсам в домене такого типа применяется полное имя узла, например zeta.webatwork.com. Здесь zeta — имя индивидуального компьютера, webatwork —домен организации, а com — домен верхнего уровня. Домены верхнего уровня являются корнями иерархии DNS и потому называются *корневыми доменами* (root domain). Эти домены орга-

низуются географически на основе двухбуквенных кодов стран (*ru* для России), по типу организации (com для коммерческих организаций) и по назначению *(shop* для интерактивных магазинов).

Обычные домены, такие как microsoft.com, называются *родительскими* (parent domain), поскольку образуют корень организационной структуры. Родительские домены можно разделить на поддоменьт, которые могут использоваться для разных офисов, отделов или удаленных филиалов. Например, полное имя компьютера в офисе Microsoft в Сиэтле может быть jacob.seattle.microsoft.com, где Jacob — имя компьютера, Seattle — поддомен, a microsoft.com — родительский домен. Другое название поддомена — *дочерний домен* (child domain).

Итак, DNS — *неотъемлемая* часть технологии Active Directory, причем настолько, что фактически вы должны настроить DNS в сети перед установкой Active Directory. О работе с DNS см. главу 19. Сконфигурировав DNS, можно установить Active Directory с помощью мастера: в меню Start (Пуск) выберите команду Run (Выполнить), в поле Open (Открыть) введите **dcpromo** и щелкните OK. Если в сети нет доменов, мастер поможет создать домен и сконфигурировать в нем Active Directory. Мастер также помогает добавлять дочерние домены в существующие структуры доменов.

Примечание В оставшейся части главы Active Directory и домены Active Directory будут часто называться просто *каталогом* и *доменами,* кроме тех случаев, когда надо отличать структуры Active Directory от структур DNS или Windows NT.

Начало работы с Active Directory

Active Directory обеспечивает логическую и физическую структуру для компонентов сети. Логические структуры - это:

- домены — группакомпьютеров, совместно использующих общую БД каталога;
- **деревья доменов — один или более** доменов, **совместно** использующих непрерывное пространство имен;
- леса доменов — одно или болеедеревьев доменов, совместно использующих общую информацию каталога;

- **организационные подразделения (ОП) — подгруппа** доменов, которые часто отражают функциональную или бизнес-структуру компании;
- подсети — сетевая группа с заданной областью IP-адресов и сетевой маской;
- сайты — одна или более подсетей; используются для настройки доступа к каталогу и для репликации.

Работа с доменными структурами

Логические структуры помогают организовывать объекты каталога и управлять сетевыми учетными записями и общими ресурсами. Логические структуры включают леса доменов, деревья доменов, домены и ОП. Сайты и подсети, с другой стороны, — физические структуры, которые помогают планировать физическую структуру сети. Физические структуры формируют сетевые связи и физические границы вокруг сетевых ресурсов.

Понятие домена

Домен Active Directory — это просто группа компьютеров, совместно использующих общую БД. Имена доменов Active Directory должны быть уникальны. Например, у вас не может быть двух доменов microsoft.com, но может быть родительский домен microsoft.com с дочерними доменами seattle.microsoft.com и ny.microsoft.com. Если домен является частью закрытой сети, имя, присвоенное новому домену, не должно конфликтовать ни с одним из существующих имен доменов в этой сети. Если домен — часть глобальной сети Интернет, то имя нового домена не должно конфликтовать ни с одним из существующих имен доменов в Интернете. Чтобы гарантировать уникальность имен в Интернете, имя родительского домена нужно зарегистрировать. Регистрацией домена можно управлять через InterNIC (http://www.mternic.net) или другую полномочную регистрационную организацию.

У каждого домена собственные политики безопасности и доверительные отношения с другими доменами. Домены могут охватывать более одного физического расположения, т. е. домен может состоять из множества сайтов, а сайты — обладать множеством подсетей. В БД каталога домена хранятся объекты, определяющие учетные записи для пользователей,

групп и компьютеров, а также **общие** ресурсы, например принтеры и папки.

Примечание Об учетных записях пользователей и групп см. главу 7. 06 учетных записях компьютеров и разных типах компьютеров, используемых доменами Windows 2000, см. раздел «Работа с доменами Active Directory».

Понятие лесов доменов и деревьев доменов

Каждый домен Active Directory обладает DNS-именем типа microsoft.com. Домены, совместно использующие данные каталога, образуют *лес* (forest). Имена доменов в лесу могут быть *несмежными* (discontiguous) или *смежными* (contiguous) в иерархии имен DNS.

Домены, обладающие смежной структурой имен, называют деревом доменов (рис. 5-1). На рисунке у корневого домена msnbc.com есть два дочерних — seattle.msnbc.com и ny.msnbc.com. У этих доменов в свою очередь тоже есть поддомены. Все эти домены являются частью одного дерева, так как у них один и тот же корневой домен.

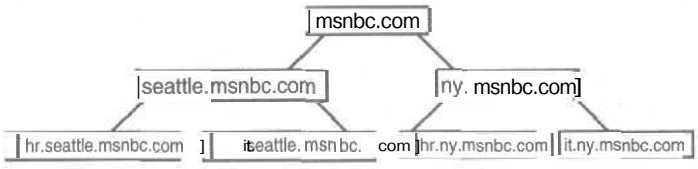


Рис. 5-1. Домены **в одном** дереве совместно используют смежную структуру имен.

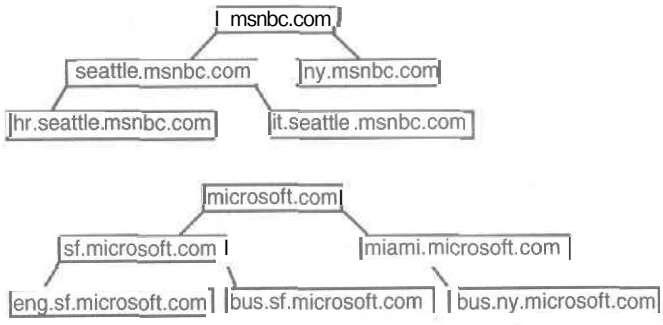


Рис. 5-2. Разные **деревья** в лесу обладают несмежными структурами имен.

Если у доменов леса несмежные DNS-имена, они образуют отдельные деревья доменов в лесу. В лес можно включить одно или несколько деревьев доменов (рис. 5-2). На рисунке домены msnbc.com и microsoft.com образуют корни отдельных деревьев доменов в одном лесу.

Для доступа к структурам домена служит Active Directory Domains And Trusts (рис. .1-3). К этой оснастке для Microsoft Management Console (MMC) можно обратиться из меню Administrative Tools. Для каждого корневого домена отображаются отдельные записи.

Рис. 5-3. Active Directory Domains And Trusts служит для работы с доменами, деревьями и лесами.

Понятие организационных подразделений

Организационные подразделения (ОП) — это подгруппы в доменах, которые часто отражают функциональную или бизнес-структуру организации. Можно воспринимать ОП как логические контейнеры, в которые помещаются учетные записи, общие ресурсы и другие ОП. Например, вы можете создать в домене microsoft.com подразделения HumanResourses, IT, Marketing. Потом эту схему можно расширить, так чтобы она содержала дочерние подразделения. Дочерними ОП для Marketing могут быть OnlineSales, ChannelSales и PrintSales.

В ОП можно поместить объекты только из родительского домена. Например, ОП из домена seattle.microsoft.com содержат объекты только этого домена. Добавить туда объекты из

ny.microsoft.com нельзя, но вы можете создать отдельные ОП, отражающие бизнес-структуру seattle.microsoft.com.

ОП очень удобны при формировании функциональной или бизнес-структуры организации. Но это не единственная причина применения ОП.

- ОП позволяют определять групповую политику для небольшого набора ресурсов в домене, не применяя ее ко всему домену. Это помогает устанавливать и управлять групповыми политиками на надлежащем уровне.
- ОП создают меньшие, более управляемые представления объектов каталога в домене. Это помогает эффективнее управлять ресурсами.
- ОП позволяют делегировать полномочия и контролировать административный доступ к ресурсам домена. Это помогает задавать пределы полномочий администраторов в домене. Вы можете передать пользователю А административные полномочия только для одного ОП. Б то же время можно передать пользователю В административные полномочия для всех ОП в домене.

ОП представлены в виде папок в Active Directory Users And Computers (рис. 5-4.) Эту оснастку MMC также можно вызвать из меню Administrative Tools.

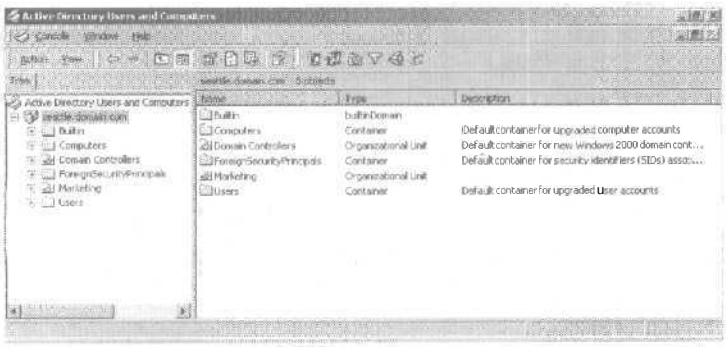


Рис. 5-4. Active Directory Users And Computers позволяет управлять пользователями, **группами,** компьютерами и ОП.

Понятие сайтов и подсетей

Сайт — это группа компьютеров в одной или более подсетей TP, используемая для планирования физической струк-

туры сети. Планирование сайтов не зависит от логических структур домена, и поэтому лет нужды связывать физическую и логическую структуру домена в сети. Active Directory позволяет создать множество сайтов в одном домене или один сайт, охватывающий множество доменов. Также нет связи между областями IP-адресов и пространством имен домена.

Вообще подсеть можно представить как группу сетевых адресов. В отличие от сайтов, способных охватывать множество областей IP-адресов, подсети обладают заданной областью IP-адресов и сетевой маской. Имена подсетей показываются в форме *сеть/битоваямаска,* например 192.168.19.9/32, где сетевой адрес 192.168.19.0 и сетевая маска 255.255.255 скомбинированы в имя подсети 192.168.19.9/32.

Примечание Вам не нужно знать, как создается имя подсети. Чаще всего вы вводите сетевой адрес и сетевую маску, а затем Windows 2000 сама генерирует имя подсети.

Компьютеры приписываются сайтам в зависимости от местоположения в подсети или наборе подсетей. Если компьютеры в подсетях могут взаимодействовать по сети на достаточно высоких скоростях, их называют *хорошо связанными* (well connected). В идеале сайты состоят из подсетей и хорошо связанных компьютеров. Если скорость обмена между подсетями и компьютерами низка, может потребоваться создать несколько сайтов. Хорошая связь дает сайтам некоторые преимущества.

- Когда клиенты входят в домен, процесс аутентификации сначала находит контроллеры домена в сайте клиента, т. е. по возможности первыми опрашиваются локальные контроллеры домена, что локализует сетевой трафик и ускоряет аутентификацию.
- Информация каталога реплицируется чаще *внутри* сайтов, чем *между* сайтами. Это снижает межсетевой трафик, вызванный репликацией, и гарантирует, что локальные контроллеры доменов быстро получат обновленную информацию. Вы можете настроить порядок репликации данных каталога, используя связи сайтов. Например, можно определить сервер-плацдарм для репликации между сайтами. В итоге основная часть нагрузки от репликации между сайтами ляжет на сервер-плацдарм, а не па любой доступный сервер сайта.

Сайты и подсети настраиваются в консоли Active Directory Sites And Services (рис. 5-5), которая вызывается из меню Administrative Tools. Поскольку это и оснастка MMC, вы можете добавить ее в любую собственную консоль.

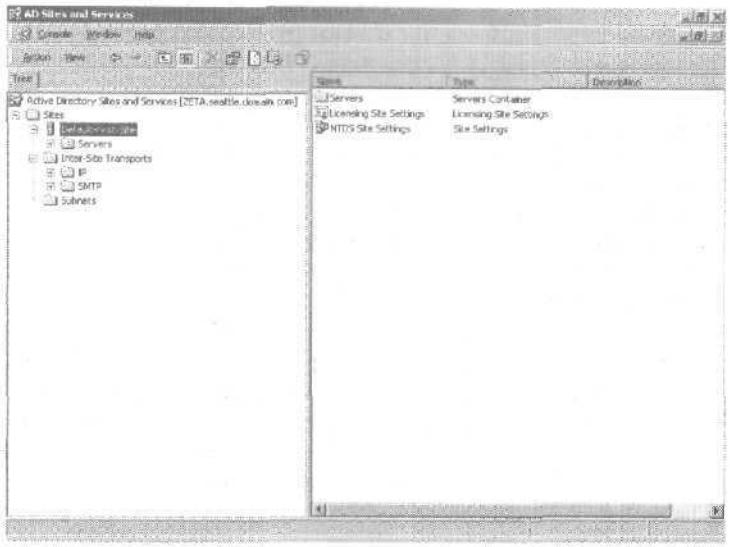


Рис. 5-5. Active Directory Sites And Services позволяет управлять сайтами и подсетями.

Работа с доменами Active Directory

Хотя и Active Directory, и DNS должны конфигурироваться в сети Windows 2000, у доменов Active Directory и доменов DNS разное назначение. Домены Active Directory помогают управлять учетными записями, ресурсами и защитой. Домены DNS формируют иерархию доменов, которая главным образом служит для разрешения имен. Windows 2000 использует DNS для преобразования имен узлов, например microsoft.com, в числовые адреса TCP/IP типа 207.149.110.52. О DNS и доменах DNS см. главу 19.

Active Directory спроектирована для работы не только с Microsoft Windows 2000, но и с Windows 95/98/NT. Если установлено ПО клиента, системы Windows 95/98/NT работают в сети как клиенты Active Directory. Системы Windows NT (и Windows 95 или более поздние без ПО клиента Active

Directory) работают в сети, как если бы они были в домене Windows NT, если это допускает рабочий режим домена Active Directory и домен Windows NT сконфигурирован.

Использование Windows 2000 с Active Directory

Windows 2000 Professional и серверы Windows 2000 могут задействовать преимущества Active Directory в полной мере. Системы на базе Windows 2000 Professional работают в сети как клиенты Active Directory и могут использовать отношения с транзитивным доверием, существующие в дереве или лесу доменов. Транзитивное доверие устанавливается автоматически в соответствии со структурой леса и разрешений, определенных в лесу. Эти отношения позволяют авторизованным пользователям получать доступ к ресурсам в любом домене леса.

Системы с Windows 2000 Server предоставляют службы для других систем и могут действовать, как контроллер домена или рядовой сервер. Контроллер домена в отличие от рядового сервера выполняет Active Directory. Рядовые серверы становятся контроллерами после установки Active Directory; контроллеры понижаются до рядовых серверов после удаления Active Directory, Оба процесса выполняет мастер установки Active Directory.

Домены могут обладать одним или несколькими контроллерами. Когда в сети несколько контроллеров, они реплицируют между собой данные каталога по модели репликации с несколькими хозяевами, которая позволяет каждому контроллеру обрабатывать изменения каталога, а затем реплицировать их на другие контроллеры.

Благодаря структуре с несколькими хозяевами, все контроллеры по умолчанию обладают равной ответственностью. Впрочем, вы можете дать некоторым контроллерам домена приоритет над другими в определенных задачах, например, создать сервер-плацдарм, который обладает приоритетом мри репликации данных каталога на другие сайты. Кроме того, некоторые задачи лучш е выполнять на выделенном сервере. Сервер, обрабатывающий такой тип задания, называется *хозяином операций* (operations master). Существует пять монопольных операций, которые можно назначить разным контроллерам домена (см. раздел «Понятие ролей хозяина операций»).

Все компьютеры с Windows 2000, присоединенные к домену, обладают учетными записями компьютера. Как и другие ресурсы, они хранятся в виде объектов в Active Directory. Учетные записи компьютера служат для управления доступом к сети и ее ресурсам. Компьютер получает доступ к домену по своей учетной записи, которая аутентифицируется до того, как компьютер сможет получить доступ в сеть.

Совет Windows 2000 использует глобальный каталог Active Directory для аутентификации входа в систему и пользователей, и компьютеров. Если глобальный каталог недоступен, только участники группы Domain Admins могут войти в домен (см. раздел «Понятие структуры каталога»).

Active Directory и Windows NT

Все компьютеры с Windows NT должны обладать учетными записями перед тем, как они смогут присоединиться к домену. Для поддержки Windows NT предусмотрено два рабочих режима Active Directory.

- В смешанном режиме каталог может поддерживать и домены Windows 2000. и домены Windows NT.
- В основном режиме каталог поддерживает только домены Windows 2000,

Смешанный **режим** работы домена

Режим домена определяется при установке Active Directory на первый контроллер. Если вы обновляете систему с Windows NT до Windows 2000, главный контроллер домена (primary domain controller, PDC) обычно обновляется до Windows 2000. PDC обновляется, чтобы гарантировать, что он будет первым контроллером в домене и что существующие объекты диспетчера учетных записей безопасности (Security Account Manager, SAM) скопируются из реестра в новое хранилище данных в Active Directory. При обновлении PDC и установке Active Directory выберите *смешанный* (mixed) режим, чтобы гарантировать, что остальные компьютеры с Windows NT смогут продолжить работу в домене.

В смешанном режиме компьютеры, настроенные для работы с доменами Windows NT, получают доступ к сети, как если бы они по-прежнему работали в домене Windows NT. Это могут быть компьютеры с Windows 9*x*, на которых не запущен клиент Active Directory, рабочие станции и серверы

Windows NT. Роль рабочих станций Windows NT неизменна, а вот серверы Windows NT воспринимаются несколько иначе: они могут действовать лишь как резервные контроллеры домена (backup domain controller, BDC) или рядовые серверы. В домене больше не может быть PDC на базе Windows NT. Вместо этого домен Windows NT подчиняется контроллеру Windows 2000, который играет роль PDC для репликации копий службы каталогов Active Directory, доступных только для чтения, и для синхронизации изменений защиты на всех оставшихся BDC на базе Windows NT.

Контроллер домена Windows 2000, действующий как PDC, конфигурируется как хозяин операций эмулятора PDC. Вы можете в любой момент назначить эту роль другому контроллеру домена Windows 2000. Контроллер, действующий как эмулятор PDC, поддерживает два протокола аутентификации:

- **Kerberos** — стандартный Интернет-протокол для аутентификации пользователей и систем и главный механизм аутентификации для доменов Windows 2000 и Windows NT;
- диспетчер локальной сети **NT** (NT Local Area Network Manager, NTLM) — главный протокол аутентификации Windows NT.

Примечание Windows 2000 также поддерживает протоколы Secure Socket Layer/Transport Layer Security (SSL/TLS). Этот механизм аутентификации применяется на защищенных Web-серверах.

Перевод домена в основной режим работы

Обновив PDC и другие системы Windows NT до Windows 2000, можно сменить рабочий режим на основной и задействовать только ресурсы Windows 2000. Перейдя на основной режим, вы не сможете вернуться к смешанному. Поэтому используйте основной режим, только когда вы уверены, что вам не понадобится старая структура домена Windows NT или резервные контроллеры домена Windows NT.

Чтобы сменить рабочий режим, сделайте так.

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и выберите Active Directory Domains And Trusts (рис. 5-6).
2. Щелкнув правой кнопкой нужный домен, выберите Properties (Свойства),

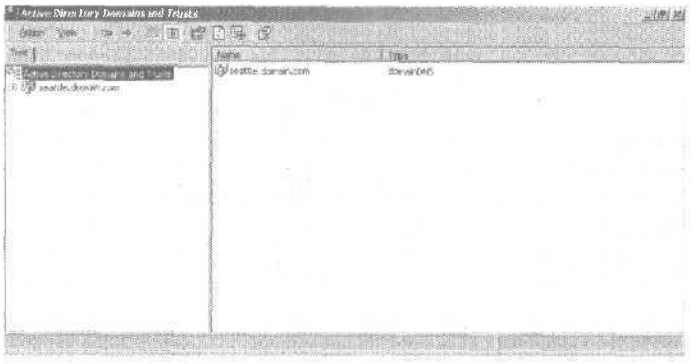


Рис. 5-6. Оснастку Active Directory Domains And Trusts можно добавить в любую консоль.

3. На вкладке General отобразится текущий режим (рис. 5-7). Если домен работает в смешанном режиме, вы можете сменить его на основной. Но это необратимое действие. Внимательно учтите все факторы перед продолжением.

Рис. 5-7. Вкладка General позволяет сменить рабочий режим домена.

4. Чтобы перейти в основной режим, щелкните Change Mode (Изменить режим), а затем Yes.

Active Directory и Windows 9x

Windows 95/98-компьютеры могут работать с Active Directory двумя способами. В зависимости от конфигурации сети они могут получать доступ к сети как часть домена Windows NT или как часть домена Active Directory.

Вход в сеть через домен Windows NT

Windows 9*x*-компьютеры получают доступ к сети как часть домена Windows NT, только если Active Directory работает в смешанном режиме и в сети доступен BDC или эмулятор PDC для аутентификации входа в систему.

В рамках эмуляции домена Windows NT системы Windows *9x* могут обращаться только к ресурсам, доступным по односторонним доверительным отношениям Windows NT, которые должны быть явно заданы администратором. Это справедливо для доступа и через контроллер Windows 2000, и через резервный контроллер Windows NT.

Вход в сеть в качестве клиента Active Directory

Системы Windows *9x* также могут получить доступ к сети как часть домена Active Directory. После установки ПО клиента Active Directory эти системы могут полностью задействовать особенности Active Directory и транзитивные доверительные отношения по всему дереву или лесу. Транзитивные доверительные отношения позволяют авторизованным пользователям автоматически получать доступ к ресурсам в любом домене дерева или леса.

Совет Транзитивные доверительные отношения автоматически конфигурируются при установке контроллера домена, и вам не обязательно их настраивать явно. Впрочем, Windows 2000 поддерживает явные доверительные отношения, и при необходимости вы можете их установить. Основные причины настройки явного доверия — обеспечить аутентификацию пользователей в другом домене или сократить маршрут доверия в сложном лесу доменов.

Установка клиентов Active Directory

1. Войдите в систему на компьютере Windows 9*x*, который хотите сконфигурировать как клиент, и вставьте установочный компакт-диск Windows 2000 Server.
2. Откройте окно Run (Запуск программы), нажав Start (Пуск), а затем Run (Выполнить).
3. Наберите **Clients\Win9X\Dsclient.exe** и щелкните OK. Или щелкните Browse (Обзор), чтобы просмотреть диск дистрибутива. В папке Clients вы найдете папку Win9X, которая должна содержать исполняемую программу клиента. Выберите эту программу, щелкните Open (Открыть), а затем — OK.
4. В ходе выполнения программа записывает несколько файлов на компьютер клиента и запускает мастер Directory Service Client Setup Wizard (рис. 5-8). Прочтите текст в окне приветствия и щелкните Next (Далее).

Рис. 5-8. Мастер помогает установить ПО клиента службы каталогов.

5. Установите ПО клиента, щелкнув Next. Мастер определит конфигурацию системы и установит нужные файлы.
6. Щелкните Finish (Готово), чтобы завершить операцию и перезагрузите компьютер.
7. В панели управления дважды щелкните Network (Сеть).

8. На вкладке Configuration (Конфигурация), выберите раздел Ethernet adapter card и щелкните Properties (Свойства). Убедитесь, что параметры TCP/IP позволяют подключиться к домену Active Directory. О настройке TCP/IP см. главу 15.
9. На вкладке Identification (Идентификация) проверьте сведения об имени компьютера и рабочей группе. Имя компьютера и рабочая группа должны быть заданы, как описано в главе 15.
10. Если вы изменили параметры, компьютер, возможно, понадобится перезагрузить. После перезагрузки войдите в систему по учетной записи с правами доступа в домен Active Directory. Вы должны получить доступ к ресурсам в домене.

Примечание Системы Windows 9x в роли клиентов не имеют учетных записей компьютеров и не отображаются в окне Network Neighborhood (Сетевое окружение), но вы можете просмотреть информацию об их сеансе связи. Запустите Computer Management, раскройте System Tools (Служебные программы), Shared Folders (Общие папки) и выберите Sessions (Сеансы) — отобразятся текущие сеансы связи пользователей и компьютеров. Об общих ресурсах см. главу 13.

Понятие структуры каталога

Active Directory построена на множестве технологий. Данные каталога предоставляются пользователям и компьютерам через хранилища и глобальные каталоги (ГК). Хотя большинство задач Active Directory отражается в хранилище данных, ГК не менее важны, потому что используются для входа в систему и поиска информации. Фактически, если ГК недоступен, обычные пользователи не смогут войти в домен.

Доступ и распространение данных Active Directory обеспечивается средствами протоколов доступа и репликации. Первые позволяют клиентам связываться с компьютерами, выполняющими Active Directory. Репликация нужна для распространения обновленных данных на контроллеры. Хотя репликация с несколькими хозяевами — главный метод рас-

пространения обновлений, некоторые изменения могут выполнять только отдельные контроллеры — *хозяева операций.*

Хранилище данных

Хранилище содержит сведения о таких объектах, как учетные записи, общие ресурсы, ОП и групповые политики. Другое название хранилища данных — *каталог,* как называют и саму службу Active Directory.

Контроллеры доменов хранят каталог в файле NTDS.DIT. Его местоположение определяется при установке Active Directory, но это должен быть диск в формате NTFS для Windows 2000. Данные каталога можно сохранить и отдельно от основного хранилища. Например, так можно хранить групповые политики, сценарии и другую информацию из общего системного тома (SYSVOL).

Поскольку хранилище — контейнер для объектов, предоставление информации каталога в совместное пользование называют *публикацией* (publish). Например, открывая принтер в сети, вы его публикуете; публикуется информация об общей папке и т. п.

Контроллеры доменов реплицируют большинство изменений в хранилище по схеме с несколькими хозяевами. Администратору небольшой или среднего размера организации редко требуется управлять репликацией хранилища. В конце концов репликация осуществляется автоматически, но вы вправе настроить ее под сетевую архитектуру организации.

Реплицируются не все данные каталога, а **лишь:**

- данные домена — информация об объектах в домене, включая объекты учетных записей, общих ресурсов, ОП и групповых политик;
- данные конфигурации — сведения о топологии каталога: список всех доменов, деревьев и лесов, а также местоположения контроллеров и серверов ГК;
- данные схемы — информация обо всех объектах и типах данных, которые могут храниться в каталоге; стандартная схема Windows 2000 описывает объекты учетных записей, объекты общих ресурсов и др.; вы можете расширить ее, определив новые объекты и атрибуты или добавив атрибуты для существующих объектов.

Глобальный каталог

ГК позволяет входить в сеть, предоставив информацию об участии в универсальной группе. ГК также обеспечивает поиск в каталоге по всем доменам леса. Контроллер, выполняющий роль сервера **ГК,** хранит полную реплику всех объектов в каталоге для своего домена и частичную реплику объектов остальных доменов леса.

Примечание Частичные реплики используются потому, что для входа в систему и поиска нужны лишь некоторые свойства. Для формирования частичной реплики по сети нужно передать меньше информации, что снижает сетевой трафик репликации.

По умолчанию сервером ГК становится первый контроллер домена. Поэтому, если в домене только один контроллер, то сервер ГК и контроллер домена — один и тот же сервер. Вы также вправе расположить ГК на другом контроллере, чтобы сократить время ожидания ответа при входе в систему и ускорить поиск. Рекомендуется создать по одному ГК в каждом сайте домена.

Контроллеры, хранящие ГК, должны иметь скоростную связь с контроллерами — хозяевами инфраструктуры. Хозяин инфраструктуры — одна из пяти ролей хозяина операций, которую можно назначить контроллеру домена. В домене хозяин инфраструктуры отвечает за обновление ссылок объектов. Он сравнивает свои данные с данными ГК, находит устаревшие ссылки и запрашивает обновленные сведения из ГК. Затем он реплицирует изменения на остальные контроллеры в домене. О ролях хозяина операций см. раздел «Понятие ролей хозяина операций».

Если в домене только один контроллер, вы можете назначить роль хозяина инфраструктуры и ГК одному контроллеру домена. Но если в домене два или более контроллеров, ГК и хозяин инфраструктуры должны быть на разных контроллерах. Иначе хозяин инфраструктуры не найдет устаревших данных и в итоге никогда не будет реплицировать изменения. Единственное исключение — когда все контроллеры домена хранят ГК. Тогда неважно, какой из них — хозяин инфраструктуры.

Одна из ключевых причин добавления ГК в домен — гарантировать, что каталог доступен для обслуживания входа в сеть и запросов поиска. Опять же, если в домене только один

ГК и каталог недоступен, обычные пользователи не смогут войти в сеть и искать объекты. Такая возможность останется только у членов группы Domain Admins (Администраторы домена).

Поиск в ГК очень эффективен, поскольку ГК содержит информацию об объектах во всех доменах леса. Это позволяет обслуживать запросы поиска каталога в локальном домене, а не обращаться в домен в другой части сети. Локальное разрешение запросов снижает нагрузку на сеть и обычно ускоряет ответ.

Внимание! Если вход в систему замедлился или пользователи долго ждут ответа на запрос, создайте дополнительные ГК. Однако большое количество ГК влечет передачу большего объема данных по сети.

Репликация и Active Directory

В каталоге хранится три типа информации: данные домена, данные схемы и данные конфигурации.

Данные домена реплицируются на все контроллеры отдельного домена. Информация схемы и конфигурации реплицируется на все домены дерева или леса. Кроме того, в ГК реплицируются все объекты индивидуального домена и подмножество свойств объектов всего леса.

Это означает, что контроллеры доменов хранят и реплицируют информацию схемы для дерева или леса, информацию конфигурации для всех доменов дерена или леса и все объекты каталога и свойства для соответствующих доменов.

Чтобы понять репликацию, рассмотрим такой сценарий настройки новой сети.

1. Вы начинаете с установки первого контроллера в домене А. Этот сервер — единственный контроллер домена и также храпит ГК. Репликация в такой сети не происходит, поскольку нет других контроллеров.
2. Вы устанавливаете второй контроллер в домене А, и начинается репликация. Чтобы убедиться, что данные реплицируются правильно, можно назначить один контроллер хозяином инфраструктуры, а другой — сервером ГК. Хозяин инфраструктуры следит за обновлениями ГК и запрашивает их для измененных объектов. Оба этих контроллера также реплицируют данные схемы и конфигурации.

3. Вы устанавливаете третий контроллер в домене А, на котором нет ГК. Хозяин инфраструктуры следит за обновлениями ГК, запрашивает их для измененных объектов, а затем реплицирует изменения на третий контроллер домена. Все три контроллера также реплицируют данные схемы и конфигурации.
4. Вы создаете новый домен Б и добавляете в него контроллеры. Серверы ГК в домене А и домене Б реплицируют все данные схемы и конфигурации, а также подмножество данных домена из каждого домена. Репликация в домене А продолжается, как описано выше, плюс начинается репликация внутри домена Б.

Active Directory и LDAP

Упрощенный протокол доступа к каталогам (Lightweight Directory Access Protocol, LDAP) — стандартный протокол Интернет-соединений в сетях TCP/IP. LDAP спроектирован специально для доступа к службам каталогов с минимальными издержками. LDAP также определяет операции, используемые для запроса и изменения информации каталога.

Клиенты Active Directory применяют LDAP для связи с компьютерами, выполняющими Active Directory, при каждом входе в сеть или поиске общих ресурсов. LDAP можно использовать и для управления Active Directory.

LDAP — открытый стандарт, который могут применять и другие службы каталога. Это делает взаимосвязь каталогов проще и значительно упрощает переход с других служб каталогов на Active Directory. Вы можете также использовать интерфейсы служб Active Directory (Active Directory Service Interfaces, ADSI) для повышения совместимости. ADSI поддерживает стандартные API-интерфесы для LDAP, совместимые с Интернет-стандартом RFC 1823. Вы можете использовать ADSI совместно с сервером сценариев Windows (Windows Script Host, WSH) для управления объектами Active Directory из сценариев.

Понятие ролей хозяина операций

Хозяин операций решает задачи, которые неудобно параллельно выполнять на нескольких хозяевах. Существует пять ролей хозяина операций — вы можете назначить их одному

или более контроллерам доменов, Определенные роли должны быть уникальны на уровне леса, для других достаточно уровня домена. Роли хозяина операций таковы.

- **Хозяин схемы** контролирует обновления/изменения схемы каталога. Для обновления схемы каталога вы должны обладать доступом к хозяину схемы. В лесу может быть только один хозяин схемы.
- **Хозяин именования доменов** контролирует добавление/удаление доменов в лесу. Чтобы добавить/удалить домен, вы должны обладать доступом к хозяину именования доменов. В лесу может быть только один хозяин именования доменов.
- **Хозяин относительных идентификаторов** выделяет относительные идентификаторы контроллерам доменов. Каждый раз при создании объекта пользователя, группы или компьютера контроллеры назначают уникальный идентификатор безопасности объекту. Идентификатор безопасности состоит из префикса идентификатора безопасности домена и соответствующего уникального идентификатора, который был выделен хозяином относительных идентификаторов. В каждом домене леса должен быть один хозяин относительных идентификаторов.

  Примечание В комплекте ресурсов Windows 2000 есть программа MOVETREE.EXE для перемещения объектов между доменами. При работе с этой утилитой перемещение должно быть инициировано на хозяине относительных идентификаторов домена, который содержит перемещаемый объект.

- **Эмулятор PDC** в смешанном режиме домена действует как главный контроллер домена Windows NT. Он аутентифицирует вход в Windows NT, обрабатывает изменения пароля и реплицирует обновления на BDC. Вы должны назначить по одному эмулятору PDC в каждый домен леса.
- **Хозяин инфраструктуры** обновляет ссылки объектов, сравнивая свои данные каталога с данными ГК. Если данные устарели, он запрашивает из ГК обновления и реплицирует их на остальные контроллеры в домене. Вы должны назначить по одному хозяину инфраструктуры в каждый домен леса.

Обычно роли хозяина операций назначаются автоматически, но вы можете их переназначить. При установке новой сети первый контроллер первого домена получает все роли хозяев операций. Если вы позднее создадите новый дочерний домен или корневой домен в новом дереве, первому контроллеру домена также автоматически назначаются роли хозяина операций. В новом лесу доменов контроллеру домена назначаются все роли хозяина операций. Если новый домен создается в том же лесу, его контроллеру назначаются роли хозяина относительных идентификаторов, эмулятора PDC и хозяина инфраструктуры. Роли хозяина схемы и хозяина именования доменов остаются у первого домена леса.

Если и домене только один контроллер, он выполняет все роли хозяев операций. Если в вашей сети один сайт, стандартное расположение хозяев операций оптимально. Но по мере добавления контроллеров домена и доменов может потребоваться переместить роли хозяев операций на другие контроллеры доменов.

Если в домене два или более контроллеров, сконфигурируйте два контроллера доменов для выполнения ролей хозяина операций. Например, можно назначить один контроллер домена основным хозяином операций, а другой — запасным. Запасной хозяин используется при отказе основного. Убедитесь, что контроллеры доменов — прямые партнеры по репликации и соединены скоростным каналом связи.

По мере роста структуры доменов можно разнести роли хозяина операций по отдельным контроллерам. Это ускорит отклик хозяев операций на запросы. Всегда тщательно планируйте ролевые обязанности будущего контроллера домена.

Примечание Две роли, которые не следует разбивать, — хозяин схемы и хозяин именования доменов. Всегда назначайте их одному серверу. Для наибольшей эффективности желательно, чтобы хозяин относительных идентификаторов и эмулятор PDC также были на одном сервере, хотя при необходимости эти роли можно разделить. Так, в большой сети, где большие нагрузки снижают быстродействие, хозяин относительных идентификаторов и эмулятор PDC должны быть размещены на разных контроллерах. Кроме того, хозяин инфраструктуры не должен быть помещен на контроллере домена, хранящем ГК (см. раздел «Глобальный каталог»).

Глава 6

Основы администрирования Active Directory

Ежедневно с помощью службы Active Directory вы будете создавать учетные записи компьютеров, подключать их к домену и т, д. Здесь вы изучите средства управления Active Directory и методы управления компьютерами, контроллерами домена и организационными подразделениями (ОП).

Средства управления службами Active Directory

Для управления Active **Directory предназначены** средства **администрирования и поддержки.**

Средства администрирования Active Directory

Выполнены в виде оснасток консоли MMC. Инструменты управления Active Directory:

- Active Directory Users and Computers (Active Directory — пользователи и компьютеры) позволяет управлять пользователями, группами, компьютерами и ОП;
- Active Directory Domains and Trusts (Active Directory — домены и доверие) служит для работы с доменами, деревьями доменов и лесами доменов;
- Active Directory Sites and Services (Active Directory — сайты и службы) позволяет управлять сайтами и подсетями.

В Microsoft Windows 2000 Server можно добавить соответствующие оснастки в любую собственную консоль или получить доступ к средствам напрямую из меню Administrative Tools (Администрирование). Если на вашем компьютере установлена другая ОС и есть доступ к домену Windows 2000,

средства не будут доступны, пока вы их не установите. Об установке этих средств см. главу 1. Вы также можете создать пакет установки ПО для средств, которые будут распространяться и устанавливаться через Active Directory.

Еще одно средство администрирования — оснастка Active Directory Schema (Схема Active Directory) — позволяет управлять и модифицировать схему каталога. Active Directory Schema поставляется с комплектом ресурсов Windows 2000 (о его установке см. главу 1).

Средства поддержки Active Directory

Active Directory Schema — одно *из* многих средств Active Directory из состава Windows 2000 Support Tools. Вот несколько средств, которые помогут сконфигурировать, управлять и устранять неполадки Active Directory (табл. 6-1).

Табл. 6-1. Краткий перечень средств поддержки Active Directory.

Средство поддержки (имя команды)	Описание
Active Directory Administration Tool (Ldp)	Осуществляет операции по протоколу Lightweight Directory Access Protocol (LDAP) в рамках Active Directory.
Active Directory Object Manager (movetree)	Перемещает объекты из одного домена ftдругой.
Active Directory Replication Monitor (Replmon)	Управляет репликацией и отслеживает ее результаты в графическом интерфейсе.
ADSI Edit	Управляет объектами в каталоге, включая каталог схемы. Позволяет настроить списки контроля доступа для объектов.
DFS File System Utility (dfsutil)	Управляет распределенной файловой системой (distributed file system, DFS) и отображает сведения о работе DPS.
Directory Services Management Tool (NTDSUTIL)	Отображает информацию о сайтах, доменах и серверах. Управляет хозяевами операций.
DNS Server Troubleshooting Tool (dnscmd)	Исследует или регистрирует записи ресурсов службы именования доменов (Domain Name Service, DNS).
Domain Manager (netdom)	Анализирует связи сайтов и доменов, а также структуру репликации.
DSACLS	Управляет списками управления доступом для объектов в Active Directory.

Табл. 6-1. *(продолжение)*

Средство поддержки (имя команды)	Описание
DSAStat	Исследует контексты именования на контроллерах домена для выявления отличий.
Replication Diagnostics Tool (Repadmin)	Управляет репликацией и отслеживает ее результаты в режиме командной строки.
Security Descriptor Check Utility (sdcheck)	Анализирует распространение, репликацию и наследование списков управления доступом.
Showaccs	Проверяет разрешения доступа пользователей к объектам Active Directory или откатывает списки управления доступом к состоянию по умолчанию.
SIDWalker	Настраивает списки управления доступом для объектов, в прошлом принадлежавших перемещенным, удаленным или «осиротевшим» учетным записям.

Средство Active Directory Users and Computers

Это главное средство администрирования Active Directory, которое используется для выполнения всех задач, связанных с пользователями, группами и компьютерами, а также управления ОП.

Запуск Active Directory Users and Computers

Для запуска Active Directory Users and Computers выберите соответствующий ярлык в меню Administrative Tools. Также можно добавить Active Directory Users and Computers как оснастку в любую собственную консоль.

1. В MMC в меню Console (Консоль) выберите Add/Remove Snap-In (Добавить/удалить оснастку). Откроется одноименное окно.
2. На вкладке Standalone (Изолированная оснастка) щелкните Add (Добавить).
3. В окне Add Snap-In Add Standalone Snap-In (Добавить изолированную оснастку) щелкните Active Directory Users and Computers, а затем Add.

Основы работы с Active Directory Users and Computers

По умолчанию Active Directory Users and Computers работает с доменом, к которому относится ваш компьютер- Вы можете получить доступ к объектам компьютеров и пользователей в этом домене через дерево консоли (рис. 6-1). Если вы не можете найти контроллер домена или домен, с которым вы хотите работать, не показан, возможно, нужно подключиться к контроллеру вашего или другого домена. Другие высокоуровневые задачи, которые вы можете выполнить из Active Directory Users and Computers, — просмотр дополнительных параметров или поиск объектов.

Получив доступ к домену в Active Directory Users and Computers, вы заметите, что доступен стандартный набор папок:

- **Builtin** — список встроенных учетных записей пользователей;
- Computers — контейнер по умолчанию для учетных записей компьютеров;
- Domain Controllers — контейнер по умолчанию для контроллеров домена;
- **Users** — контейнер по умолчанию для пользователей.

Вы также можете добавить папки для ОП. На рис. 6-1 видно, что были созданы два ОП в домене seattle.domain.com: ForeignSecurityPrincipals и Marketing.

Соединение с контроллером домена

Соединение е контроллером домена служит нескольким целям. Если после запуска Active Directory Users and Computers вы не видите объекты, вы можете связаться с контроллером домена для получения доступа к объектам пользователей, групп и компьютеров в соответствующем домене. Можете также связаться с контроллером домена, если подозреваете, что репликация выполняется неправильно и вам нужно обследовать объекты на заданном контроллере. Подключившись, вы сможете выявить несоответствия в недавно обновленных объектах.

Чтобы связаться **с** контроллером домена, сделайте так.

1. В дереве консоли щелкните правой кнопкой Active Directory Users and Computers и выберите Connect To Domain Controller (Подключение к контроллеру домена).

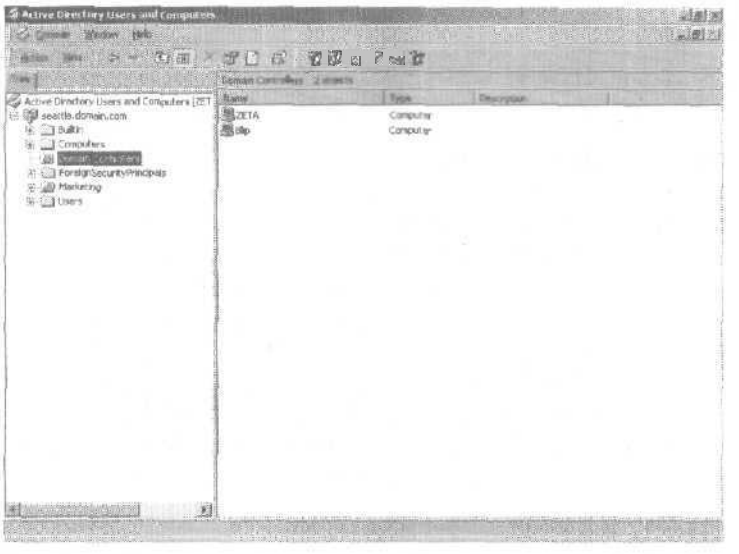


Рис. 6-1. Доступ к контроллерам домена из оснастки Active Directory Users and Computers.

2. **Вы** увидите **текущий** домен и **контроллер, с которым** работаете, в одноименном **окне** (рис. 6-2),

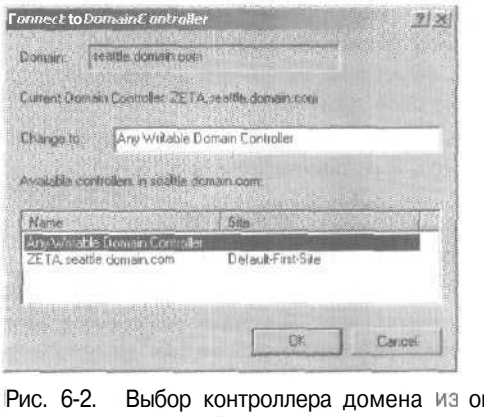


Рис. 6-2. Выбор контроллера домена из окна Connect to Domain Controller.

3. В списке Available Controllers In перечислены доступные в домене контроллеры. По умолчанию выбрано Any Wri-

table Domain Controller. Если вы выберете этот параметр, то свяжетесь с контроллером, который первым ответит на запрос. Или же выберите конкретный контроллер, с которым нужно связаться. Щелкните OK.

Соединение с доменом

Если вы имеете соответствующие права доступа, в Active Directory Users and Computers разрешается работать с любым доменом в лесу. Кот как связаться с доменом.

1. В дереве консоли щелкните правой кнопкой Active Directory Users and Computers и выберите Connect To Domain Controller.
2. В одноименном окне отображается текущий (или принятый по умолчанию) домен. Введите имя нового домена и щелкните OK. Или щелкните Browse (Обзор), а потом выберите домен в диалоговом окне.

Просмотр дополнительных параметров

Active Directory Users and Computers обладает дополнительными функциями, которые не включены по умолчанию. Чтобы просмотреть дополнительные сведения, в меню View (Вид) выберите Advanced Features (Дополнительные функции). Вы увидите три дополнительные папки:

- **ForeignSecurityPrincipals** содержитинформацию об объектах из доверенного внешнего домена; как правило, они создаются, когда объект из внешнего домена добавляется в группу в текущем домене;
- **LostAndFound** содержит «осиротевшие» объекты, которые можно удалить или восстановить;
- **System** содержит встроенные параметры системы.

Поиск учетных записей и общих ресурсов

В Active Directory Users and Computers есть внутренняя функция поиска учетных записей, общих ресурсов и других объектов каталога в текущем или указанном домене или во всем каталоге.

1. В дереве консоли щелкните правой кнопкой текущий домен или заданный контейнер, в котором хотите вести поиск, и выберите Find. Откроется окно Find Computers (рис. 6-3).

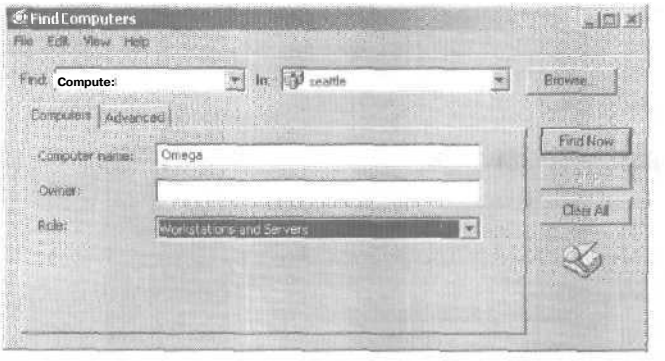


Рис. 6-3. В диалоговом окне Find Computers осуществляется поиск ресурсов в Active Directory.

2. Выберите тип поиска из списка Find:
   - Users, Contacts, And Groups (Пользователи, контакты и группы) — учетные записи пользователей и групп, а также контакты, перечисленные в службе каталогов;
   - Computers (Компьютеры) — учетные записи компьютеров по типу, имени и владельцу;
   - Printers (Принтеры) — принтеры по имени, модели и свойствам;
   - Shared Folders (Общие папки) — общие папки по имени или ключевому слову;
   - **Organizational Units** (Подразделения) **— ОП по имени.**
   - Custom **Search** (Особый поиск) — углубленный поиск или запрос по протоколу LDAP.
3. Выберите область поиска в списке In. Если вы до этого щелкнули правой кнопкой контейнер, например Computers, он выбирается по умолчанию. Чтобы искать все объекты в каталоге, выберите Entire Directory (Вся папка).
4. Введя параметры поиска, щелкните Find Now (Найти). Все совпадающие разделы отображаются внизу окна. Дважды щелкните объект для просмотра или изменения его свойств. Щелкните объект правой кнопкой для отображения меню команд управления объектом.

Примечание Тип поиска определяет, какие поля и вкладки доступны в диалоговом окне Find. Как правило, вы просто будете вводить имя искомого объекта, в поле Name, но

есть и другие параметры поиска. Например, вы можете искать цветной принтер, принтер, который может печатать на обеих сторонах листа, принтер, оснащенный скоросшивателем и т. п.

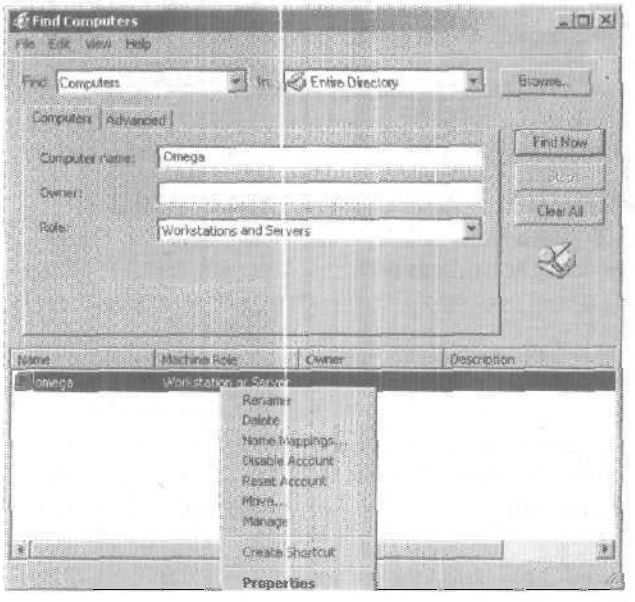


Рис. 6-4. Совпавшие с условиями поиска объекты отображаются внизу окна, и вы можете управлять ими, щелкая правой кнопкой.

Управление учетными записями компьютеров

Учетные записи компьютеров хранятся в Active Directory как объекты и могут применяться для контроля доступа к сети и ее ресурсам. Вы можете добавлять учетные записи компьютеров в любой контейнер, доступный в Active Directory Users and Computers. Лучше всего использовать контейнеры Computers, Domain Controllers и любые созданные вами ОП.

Примечание Компьютеры с Windows 9x получают доступ к сети, как клиенты Active Directory, но у них нет учетных записей компьютера. Подробнее о получении доступа к доменам Active Directory см. главу 5.

Создание учетных записей компьютера на рабочей станции или сервере

Простейший способ создания учетной записи компьютера — войти в компьютер, который вы хотите конфигурировать, и присоединиться к домену, как описано в разделе «Присоединение компьютера к домену или рабочей группе». Когда вы сделаете это, нужная учетная запись компьютера будет автоматически создана и помещена и папку Computers или Domain Controllers. Можно также заранее создавать учетные записи компьютеров в Active Directory Users and Computers.

Создание учетных записей компьютера в Active Directory Users and Computers

1. В дереве консоли Active Directory Users and Computers щелкните правой кнопкой контейнер, в котором хотите разместить учетную запись компьютера.
2. **Щелкните New (Создать), а потом — Computer (Компьютер). Откроется окно New Object — Computer (рис. 6-5).** Введите **имя** компьютера клиента.

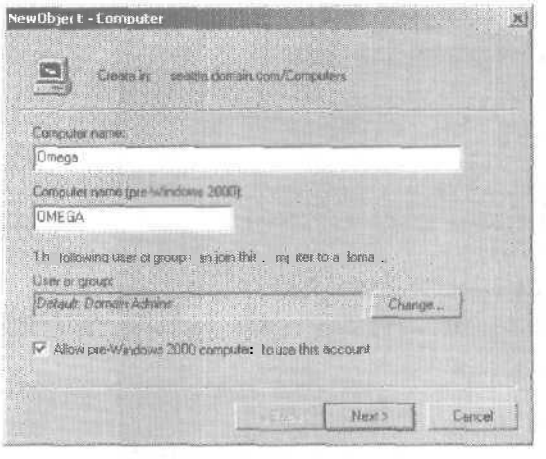


Рис. 6-5. Создавайте новые учетные записи компьютера из окна New Object-Computer. Кнопки Back и Next доступны, только если сконфигурированы службы удаленной установки (Remote Installation Services, RIS).

3. По умолчанию только члены группы **Domain** Admins **(Администраторы** домена) вправе **присоединять компьютеры**

к домену. Чтобы разрешить это другим пользователям или группам, щелкните Change (Изменить). Затем в окне Select User Or Group выберите учетную запись пользователя или группы.

Примечание Вы можете выбрать любую существующую учетную запись пользователя или группы. Это позволяет делегировать полномочия на присоединение учетной записи компьютера к домену.

4. Если эту учетную запись должны будут использовать системы Windows NT, выберите Allow Pre-Windows 2000 Computers To Use This Account.
5. Щелкните OK или Next. Если вы не настраиваете управляемый ПК, пропустите пп. 6-9. (Управляемые компьютеры — те, что можно установить удаленно. Для это требуются службы удаленной установки.)
6. Чтобы настроить управляемый компьютер, выберите This Is A Managed Computer (Это управляемый компьютер).
7. Введите глобально уникальный **идентификатор** (GUID) **в текстовом** поле **(рис. 6-6).**

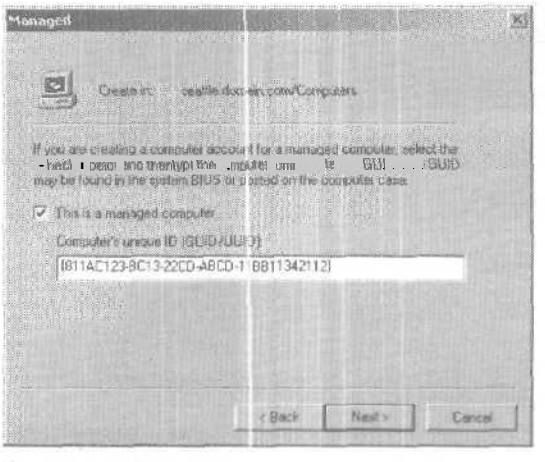


Рис. 6-6. Чтобы создать учетную запись для управляемого ПК, введите его GUID.

Примечание GUfD компьютера поставляется производителем и должен быть введен в формате {dddddddd-dddd-dddd-

dddd-dddddddddddd}, где d — шестнадцатеричная цифра, например {811AC123-BC13-22CD-ABCD-11BB11342112}. GUID указывается в наклейке снаружи или внутри корпуса компьютера, а также в BIOS.

8. Укажите, какой несущий сервер будет проводить удаленную установку, выбрав один из параметров:
   - Any Available Remote Installation Server (Любой доступный сервер удаленной установки) разрешает любому серверу удаленно устанавливать ОС на управляемый ПК;
   - The Followimg Remote Installation Server (Следующий сервер удаленной установки) разрешает удаленную установку ОС только серверу с указанным полным именем DNS.
9. Щелкните Next, а затем — Finish (Готово).

Примечание Новые компьютеры включаются в группу Domain Computers. Когда вы устанавливаете Active Directory на сервер и тот становится контроллером домена, компьютер перемещается в группу Domain Controllers. О группах см. главы 7 и 8.

Просмотр и редактирование свойств учетных записей компьютера

1. Запустите Active Directory Users and Computers.
2. В дереве консоли раскройте узел домена, щелкнув значок плюс (+) рядом с его именем.
3. Щелкните правой кнопкой нужную учетную запись и выберите Properties (Свойства). Б появившемся окне свойств можно просмотреть и изменить параметры.

Удаление, отключение и включение учетных записей компьютера

Если вам больше не нужна учетная запись какого-то компьютера, вы можете навсегда удалить ее из Active Directory или временно отключить, а позднее включить вновь.

1. Б меню Administrative Tools выберите Active Directory Users and Computers.
2. В дереве консоли щелкните контейнер, где расположена учетная запись компьютера. Затем щелкните правой кнопкой саму запись компьютера.

3. Выберите Delete (Удалить), чтобы удалить учетную запись, а затем подтвердите удаление, щелкнув Yes.
4. Выберите Disable Account (Отключить учетную запись), чтобы временно отключить учетную запись, а потом подтвердите действие, щелкнув Yes. Красный крест на значке записи указывает, что она отключена.

Внимание! Отключить используемую учетную запись невозможно. В этом случае выключите компьютер или прервите его рабочий сеанс *в* папке Sessions (Сеансы) консоли Computer Management (Управление компьютером).

5. Выберите Enable Account (Включить учетную запись), чтобы разрешить вновь использовать учетную запись.

Сброс заблокированных учетных записей компьютера

Иногда учетная запись компьютера может быть заблокирована, или компьютерный сеанс может зависнуть. Тогда сбросьте учетную запись.

1. В меню Administrative Tools выберите Active Directory Users and Computers,
2. В дереве консоли щелкните контейнер, где расположена учетная запись компьютера. Затем щелкните правой кнопкой саму запись компьютера.
3. Выберите Reset Account. Если операция удалась, вы увидите окно подтверждения. Щелкните OK.

Перемещение учетных записей компьютера

Учетные записи компьютера обычно хранятся в контейнерах Computers, Domain Com rollers или в созданных вами ОП. Вы можете переместить учетную запись в другие контейнеры.

1. В меню Administrative Tools выберите Active Directory Users and Computers.
2. В дереве консоли щелкните контейнер, где расположена учетная запись.
3. Щелкните правой кнопкой учетную запись компьютера, которую хотите переместить, и выберите Move. Откроется одноименное окно Move (рис. 6-7).
4. Щелкните узел домена, а затем — контейнер, куда хотите переместить компьютер. Щелкните OK.

Управление компьютерами

По ходу работы с Active Directory Users and Computers вы можете открыть консоль Computer Management и связаться напрямую с нужным компьютером, щелкнув правой кнопкой запись компьютера и выбрав Manage.

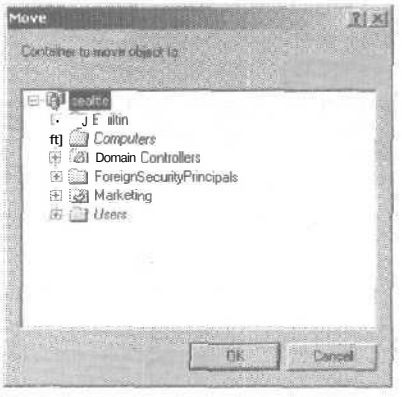


Рис. 6-7. Для перемещения учетных записей компьютеров в контейнеры служит диалоговое окно Move.

Присоединение компьютера к домену или рабочей группе

Эта операция позволяет компьютерам с Windows NT/2000 входить в сеть и получать доступ к домену. Компьютеры с Windows 95/98 не нуждаются в учетных записях компьютера и не присоединяются к сети этим методом, а настраиваются как клиенты Active Directory. Подробности см. в главе 5.

Сначала убедитесь, что на компьютере правильно установлены сетевые компоненты. Они должны были устанавливаться вместе с ОС (см. также главу 15 о настройке TCP/IP-соединсний). Если службы DHCP, WINS и DNS правильно установлены в сети, рабочим станциям не потребуются статичные IP-адреса или специальная настройка. Единственные обязательные параметры — имя компьютера и имя домена, которые вы можете задать, когда присоединяетесь к домену.

Присоединение компьютера с существующим сетевым соединением

Во время установки ОС, возможно, для компьютера было сконфигурировано сетевое соединение. Или вы могли ранее

присоединить компьютер к домену или рабочей группе. Если так, вы можете присоединить компьютер к новому домену или рабочей группе.

1. Войдите в систему на рабочей станции или сервере, который хотите сконфигурировать.
2. Откройте окно Network And Dial-Up Connections (рис. 6-8), раскрыв меню Start\Settings и выбрав Network And Dial-Up Connections (Сеть и удаленный доступ к сети),

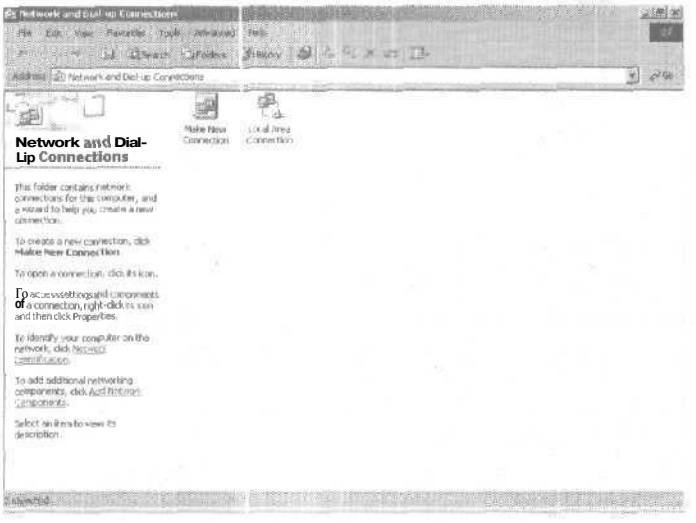


Рис. 6-8. В окне Network And Dial-Up Connections можно просмотреть и настроить сетевые соединения.

3. Если на компьютере настроены сетевые или коммутируемые соединения, они будут показаны (рис. 6-8). Дважды щелкните значок соединения для просмотра его состояния.
4. Щелкните ссылку Network Identification (Сетевая идентификация). Откроется диалоговое окно System Properties (Свойства системы) с выбранной вкладкой Network Identification (рис. 6-9).

Примечание Нельзя изменить сетевую идентификацию контроллера домена, поэтому ссылка Network Identification для него будет недоступна. Откройте Control Panel (Панель управления), дважды щелкните System (Система), а затем

в окне свойств выберите вкладку Network Identification. Вы увидите текущий сетевой идентификатор, но кнопки Network и ID Properties будут недоступны.

Рис. 6-9. Свойства и сетевой идентификатор изменяются на вкладке Network Identification.

5. Щелкните Properties.
6. Чтобы переименовать компьютер, введите новое имя в поле Computer Name (Имя компьютера), например Zeta.
7. Чтобы присоединиться к новому домену, в области Member Of (Является членом) выберите Domain (домена) и введите имя домена, например microsoft.com.
8. Чтобы присоединиться к новой рабочей группе, в панели Member Of выберите Workgroup (рабочей группы) и введите имя группы, например TestDevGroup.
9. Если вы внесли изменения, щелкните OK. В ответ на запрос введите имя и пароль учетной записи пользователя, полномочного проводить эти изменения. Снова щелкните OK.
10. Если изменения успешны, вы увидите окно подтверждения. Щелкните OK, чтобы перезагрузить компьютер.

11. Если изменения не удались, вы увидите либо сообщение об этом, либо что учетная запись уже используется. Проблема может возникнуть, когда вы изменяете имя компьютера, уже подключенного к домену, и когда у него есть активные сеансы в домене. Закройте приложения, которые могут соединяться с доменом, такие как Проводник Windows, обращающийся к общей папке в сети, и повторите процесс.

Присоединение компьютера по новому сетевому соединения

Если вы не настроили сетевую информацию во время установки ОС или вам просто нужно создать новое сетевое соединение, сделайте так.

1. Войдите на рабочую станцию или сервер, который хотите настраивать.
2. Раскройте меню Start\Settings и выберите Network And Dial-Up Connections.
3. Щелкните ссылку Network Identification, чтобы открыть окно свойств системы с выбранной вкладкой Network Identification (рис. 6-9). Как уже говорилось, этот параметр недоступен на контроллерах домена.
4. Щелкните Network ID (Идентификация), чтобы запустить мастер. Прочтите приветствие и щелкните Next.

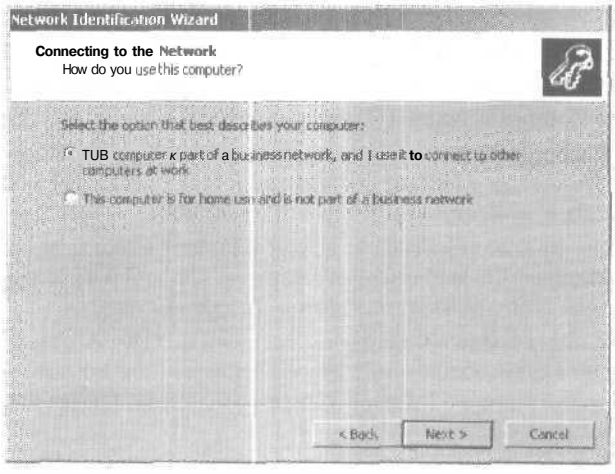


Рис. 6-Ю. Мастер Network Identification Wizard позволяет связаться с сетью для доступа к домену или рабочей группе.

5. Сетевой параметр по умолчанию — связать компьютер с сетью (рис. 6-10). Поскольку это нам и нужно, щелкните Next.
6. Чтобы присоединиться к домену, выберите My Computer Uses A Computer With A Domain (Моя организация использует сеть с доменами) и щелкните Next.
7. Чтобы присоединиться к рабочей группе, выберите **My** Computer Uses A Network Without A Domain (Моя организация использует сеть без доменов). Щелкните Next и введите имя рабочей группы, например TestDevGroup. Завершите процесс, щелкнув Next, а затем Finish. Пропустите оставшиеся шаги.
8. Вас попросят собрать информацию, которая понадобится для присоединения к домену. Вам нужно знать имя, пароль и домен учетной записи пользователя, полномочного присоединить компьютер к домену, а также целевое имя компьютера и домен. Щелкните Next.
9. Введите имя пользователя, пароль и домен административной учетной записи (рис. 6-11). Щелкните Next.

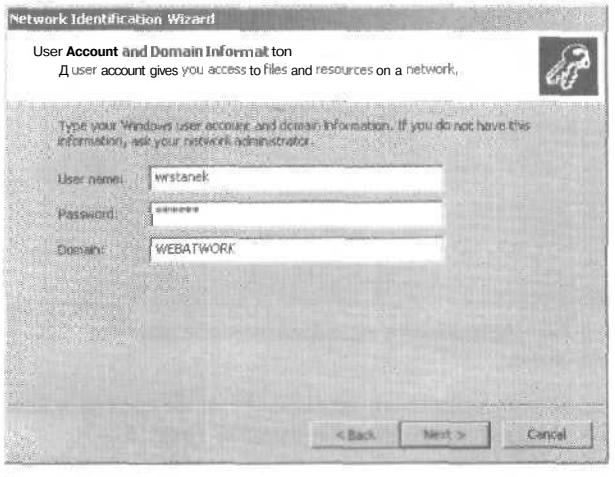


Рис. 6-11. Введите **информацию пользователя** для доступа в **сеть.**

10. Если имя компьютера и домен уже заданы и существует учетная запись для компьютера в этом домене, вы увидите запрос: хотите ли вы присоединить компьютер к до-

мену. Щелкните Yes. Иначе введите имя компьютера и домен компьютера. Затем щелкните Next.

11. Если у вас спрашивают учетную запись полномочного пользователя, введите имя пользователя, пароль и домен учетной записи пользователя, который вправе присоединять компьютер к домену. -

12. Далее у вас есть возможность уполномочить пользователя для доступа к компьютеру. Это позволит пользователю войти в систему и обратиться к ресурсам компьютера но сети. Если вы хотите сделать это, выберите Add The Following User и введите имя и домен пользователя (рис. 6-12). Или же выберите Do Not Add User At This Time. Помните, что вам может понадобиться предоставить доступ к компьютеру позже.

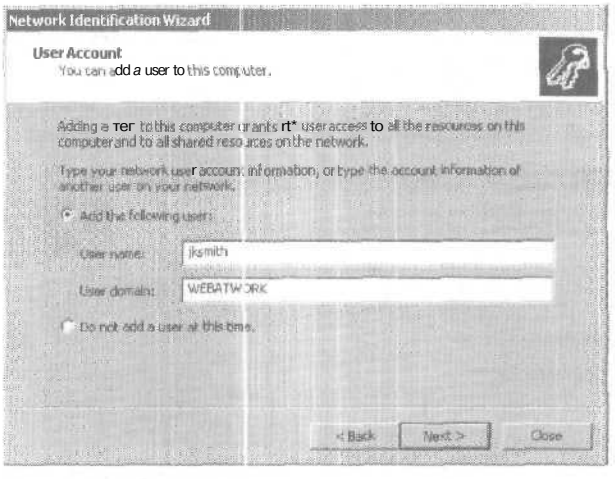


Рис. 6-12. Авторизуйте пользователя для доступа к компьютеру.

13. Если вы уполномочили пользователя па доступ к компьютеру, задайте уровень полномочий (рис. 6-13).

- Standart User — пользователь считается опытным и способен изменять параметры компьютера и устанавливать приложения; такие пользователи включаются э локальную группу Power Users (Опытные пользователи).

- **Restricted User** — обычный пользователь, способный получать доступ к компьютеру и сохранять документы. Он не может изменять параметры компьютера или устанавливать программы и включается в локальную группу Users (Пользователи).
- **Other** — позволяет включить пользователя в любую локальную группу, включая Administrators, Backup Operators (Операторы архива) и Guests (Гости).

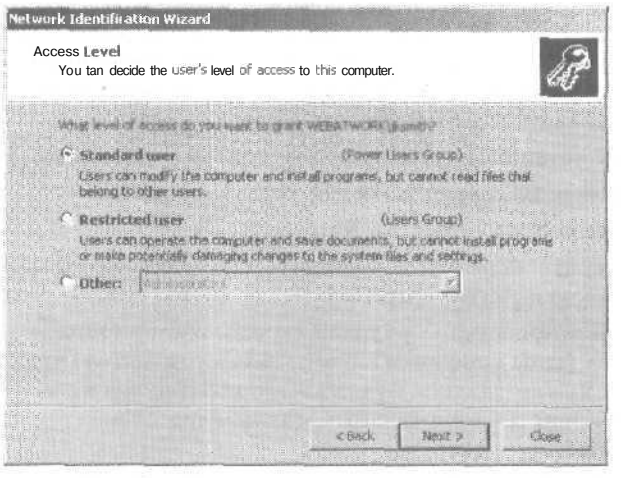


Рис. 6-13. Задайте уровень полномочий пользователя на локальном компьютере.

14. Щелкните Next, а затем Finish.

Управление контроллерами домена, ролями и каталогами

Контроллеры доменов выполняют важные задачи в доменах Active Directory. Многие из этих задач обсуждались в главе 5.

Установка и понижение контроллеров домена

Контроллер домена формируется из рядового сервера путем установки Active Directory. Если затем вы решите, что сервер больше не должен выполнять задачи контроллера, его можно понизить до уровня рядового сервера. Операции установки Active Directory и понижения контроллера похожи,

но перед выполнением этих задач проанализируйте их влияние на сеть и ознакомьтесь с главой 5.

Как там сказано, когда вы устанавливаете контроллер домена, вам может понадобиться передать роли хозяина операций и переконфигурировать структуру глобального каталога. Кроме того, перед установкой Active Directory в сети должна работать DNS, а целевой жесткий диск — иметь формат NTFS 5,0. О преобразовании дисковых форматов см. главу 10. Аналогично перед понижением контроллера нужно передать все его ключевые обязанности другим контроллерам домена, т. е. при необходимости нужно переместить глобальный каталог с сервера и передать все его роли хозяина операций.

Вот как установить или понизить контроллер домена.

1. Войдите на сервер, который хотите настроить.
2. В меню Start выберите Run.
3. Наберите **dcpromo** и щелкните OK. Запустится мастер установки Active Directory.
4. Если компьютер — рядовой сервер, мастер проведет вас через этапы установки службы каталогов Active Directory. Вам нужно указать, будет ли это контроллер нового домена или дополнительный контроллер существующего домена.
5. Если компьютер — контроллер домена, мастер проведет вас через процесс понижения контроллера домена. После понижения компьютер действует как рядовой сервер.

Просмотр и передача доменных ролей

Active Directory Users and Computers позволяет просмотреть или изменить расположение доменных ролей хозяина операций. На уровне домела вы можете работать с ролями хозяина относительных идентификаторов (Relative ID, RID), эмулятором PDC и хозяином инфраструктуры.

Примечание О роли хозяина операций см. главу 5. Для настройки роли хозяина именования служит Active Directory Domains And Trusts, а изменения роли хозяина схемы — Active Directory Schema.

Чтобы передать роль хозяина операций, сделайте так.

1. В дереве консоли щелкните правой кнопкой Active Directory Users and Computers и выберите Operations Masters. Откроется одноименное окно (рис. 6-14).

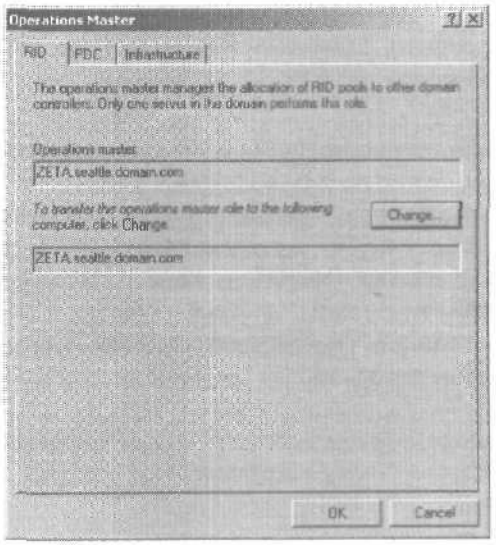


Рис. 6-14, Диалоговое окно Operations Master позволяет передать роль хозяев операций на новое место и просмотреть их текущее местоположение.

2. Вкладка RID показывает местоположение текущего хозяина относительных идентификаторов. Щелкните Change (Изменить) и выберите новый контроллер домена для передачи роли на новое место.
3. Вкладка PDC показывает местоположение текущего эмулятора PDC. Щелкните Change, а затем выберите новый контроллер домена для передачи роли на новое место.
4. Вкладка Infrastructure (Инфраструктура) показывает местоположение текущего хозяина инфраструктуры. Щелкните Change, а затем выберите новый контроллер домена для передачи роли на новое место. Щелкните OK.

Просмотр и передача роли хозяина именования домена

Вы Active Directory Users and Computers позволяет просмотреть или изменить расположение хозяина именования домена

в лесу. В Active Directory Domains And Trusts корневой уровень дерева контроля показывает выбранный домен.

Внимание! Если вам нужно связаться с другим доменом, свяжитесь с контроллером (см. раздел «Соединение с контроллером домена»). Единственное отличие в том, что вы щелкаете правой кнопкой Active Directory Domains And Trusts в дереве консоли.

Чтобы передать роль хозяина именования домена, сделайте так.

1. Запустите Active Directory Domains And Trusts.
2. В дереве консоли щелкните правой кнопкой Active Directory Domains And Trusts и выберите Operations Master. Откроется окно Change Operations Master (Изменение хозяина операций).
3. В поле Domain Naming Operations Master (Хозяин именования доменов) отображается текущий хозяин именования домена.
4. Щелкните Change, ;i затем выберите новый контроллер. Роль будет передана этому контроллеру.
5. Щелкните Close.

Просмотр и передача роли хозяина схемы

Active Directory Users and Computers позволяет просмотреть или изменить расположение хозяина схемы. Эта утилита поставляется как оснастка, доступная, когда установлен полный набор средств администрирования. Роль руководителя схемы передается так.

1. Установив средства администрирования, вы можете добавить оснастку Active Directory Schema *в* Microsoft Management Console. Щелкните Start, а затем Run.
2. Наберите mmc /a и щелкните OK.
3. В меню Console выберите Add/Remove Snap-In и щелкните Add.
4. В дереве консоли щелкните правой кнопкой Active Directory Schema и выберите Change Domain Controller (Изменение контроллера домена).
5. Выберите Any Domain Controller (Любой контроллер), чтобы позволить Active Directory выбрать нового хозяина схемы. Или выберите Specify Name (Укажите имя) и

введите имя нового хозяина схемы, например zeta.seattle.domain.com.

6. В дереве консоли щелкните правой кнопкой Active Directory Schema и выберите Operations Master (Хозяин операций). Щелкните Change.

Настройка глобальных каталогов

Глобальные каталоги (ГК) играют в сети важную роль (см. главу 5). Иногда их требуется добавлять для ускорения операций поиска, а иногда — удалять. Так, если в сайте два или более ГК, желательно оставить только один из них.

Чтобы включить/отключить ГК, сделайте так.

1. Запустите Active Directory Sites And Services.
2. В дереве консоли раскройте дерево просмотра для сайта, с которым хотите работать, щелкнув значок плюс (+) рядом с его именем.
3. Раскройте папку Servers для сайта и щелкните сервер, который хотите настроить для хранения ГК.

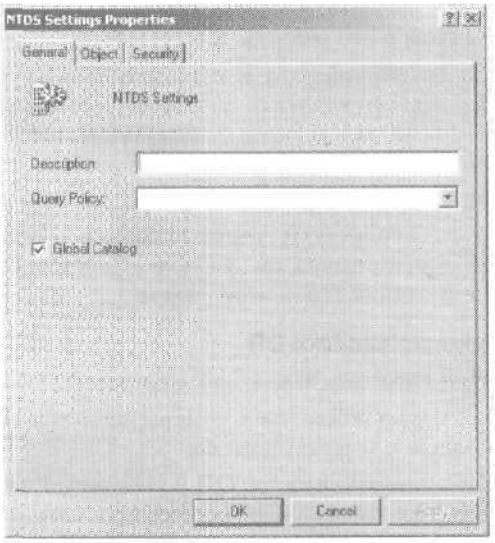


Рис. 6-15. Включение/отключение глобального каталога через NTDS-параметры сервера.

4. Щелкните правой кнопкой NTDS Settings и выберите Properties.
5. Чтобы активизировать ГК, выберите Global Catalog на вкладке General (рис. 6-15).
6. Чтобы отключить ГК, снимите флажок Global Catalog.

Управление ОП

Как говорилось в главе 5, организационные подразделения (ОП) помогают организовывать объекты, применять групповую политику в ограниченной области и т. и.

Создание ОП

Обычно ОП создают для отражения функциональной или бизнес-структуры организации. Вы можете создавать ОП как подгруппы домена или дочерние подразделения внутри существующего ОП.

ОП создается так.

1. Запустите Active Directory Users and Computers.
2. В дереве консоли раскройте узел домена, щелкнув значок плюс (+) рядом с его именем.
3. Щелкните правой кнопкой узел домена или папку существующего ОП, в которую хотите добавить ОП. Выберите в меню New (Создать), а затем — Organizational Unit (Подразделение).
4. Введите название ОП и щелкните OK.
5. Теперь вы можете перемещать учетные записи и общие ресурсы в ОП. Для примера см. раздел «Перемещение учетных записей компьютера» этой главы.

Просмотр и изменение свойств ОП

1. Запустите Active Directory Users and Computers.
2. В дереве консоли раскройте узел домена, щелкнув значок плюс (+) рядом с именем домена.
3. Щелкните правой кнопкой нужное ОП и выберите Properties. Откроется окно свойств, позволяющее просматривать и изменять параметры.

Переименование и удаление ОП

1. В Active Directory Users and Computers щелкните правой кнопкой папку ОП, с которым хотите работать.
2. Чтобы удалить ОП, выберите Delete (Удалить). Затем *подтвердите* действие, *щелкнув* Yes.
3. Чтобы переименовать ОП, выберите Rename (Переименовать). Введите новое имя для ОП и нажмите Enter.

Перемещение ОП

1. В Active Directory Users and Computers щелкните правой кнопкой папку ОП, которое хотите переместить, и выберите Move (*Переместить*).
2. В окне Move **щелкните узел** домена, а затем — **контейнер, куда хотите** переместить **ОП. Щелкните ОК.**

Глава 7

Понятие учетных записей пользователей и групп

Управление учетными записями — одна из основных задач администратора Windows 2000. В главе 3 речь шла об учетных записях компьютеров. В этой главе мы рассмотрим учетные записи пользователей и групп. Первые позволяют индивидуальным пользователям входить в сеть и получать доступ к сетевым ресурсам. Вторые применяются для управления ресурсами нескольких пользователей. Разрешения и привилегии, назначаемые пользователям и группам, определяют, какие действия могут выполнять пользователи, а также к каким компьютерным системам и ресурсам они имеют доступ.

Не предоставляйте пользователям широкого доступа к ресурсам: вы должны сбалансировать их потребности в ресурсах, связанных с определенным видом работы, с вашей потребностью защитить уязвимые ресурсы или конфиденциальные данные. Так, не стоит давать доступ к сведениям о зарплатах всем сотрудникам компании. Следовательно, нужно убедиться, что доступ к этой информации имеют лишь те, кому она нужна.

Модель безопасности Windows 2000

Доступ к сетевым ресурсам контролируется с помощью компонентов модели безопасности Windows 2000.

Протоколы аутентификации

Процесс аутентификации в Windows 2000 разделен на два этапа: интерактивный вход в систему и сетевая аутентификации.

Интерактивный вход аутентифицирует пользователя, подтверждая его подлинность на локальном компьютере, и откры-

вает доступ к службе каталогов Active Directory. Впоследствии всякий раз, когда пользователь обращается к сетевым ресурсам, сетевая аутентификация позволяет определить, есть ли у него на то разрешение.

Windows 2000 поддерживает множество протоколов аутентификации. Вот ключевые протоколы.

- Kerberos V 5 — стандартный Интернет-протокол аутентификации пользователей и систем. Это основной механизм аутентификации в Windows 2000.
- NT LAN Manager (NTLM) — основной протокол аутентификации в Windows NT. Служит для аутентификации компьютеров в домене Windows NT.
- **Secure Socket Layer/Transport Layer Security (SSL/TLS)** — основной механизм аутентификации, используемый при входе на защищенные Web-серверы.

Главная особенность модели аутентификации Windows 2000 — поддержка однократного ввода пароля для входа в систему.

1. Пользователь входит в домен, вводя имя и пароль или вставляя смарт-карту в считывающее устройство.
2. Процесс интерактивного входа аутентифицирует доступ пользователя- Для локальной учетной записи реквизиты аутентифицируются локально, и пользователю предоставляется доступ к локальному компьютеру. Для доменной учетной записи реквизиты аутентифицируются в Active Directory, и пользователь получает доступ к сетевым ресурсам.
3. Теперь пользователь может аутентифицироваться на любом компьютере в домене посредством сетевой аутентификации. Для доменных учетных записей сетевая аутентификация проходит автоматически (пароль вводится лишь раз). Пользователи с локальными учетными записями должны предоставлять имя и пароль при каждом обращении к сетевому ресурсу.

Управление доступом

Active Directory основана на объектах. Пользователи, компьютеры, группы, общие ресурсы и многие другие элементы — все определены как объекты. Управление доступом к этим объектам основано на дескрипторах безопасности, которые:

- перечисляют пользователей и группы, имеющие доступ к объектам;
- указывают разрешения, назначенные пользователям и группам;
- записывают события, аудит которых включен для объектов;
- определяют владельцев объектов.

Отдельные записи в дескрипторе безопасности называют записями управления доступом (access control entry, ACE). Объекты Active Directory могут наследовать ACE от родительских объектов, т. е. разрешения родительского объекта могут применяться к дочернему. Например, все участники группы Domain Admins (Администраторы домена) наследуют разрешения, предоставленные этой группе.

При работе с ACE помните следующее:

- ACE по умолчанию создаются с включенным наследованием;
- наследование происходит сразу после записи ACE;
- все записи управления доступом содержат информацию, указывающую, было ли разрешение унаследовано или явно назначено соответствующему объекту.

Различия между учетными записями пользователей и групп

Windows 2000 содержит учетные записи пользователей и групп (в которые могут входить пользователи). Учетные записи пользователей предназначены отдельным лицам, а учетные записи групп — чтобы упростить управление множеством пользователей. Вы можете войти в систему по учетной записи пользователя, но не по записи группы. Учетные записи групп обычно называют просто *группами*.

Учетные записи пользователей

В Windows 2000 определены два тина учетных записей пользователя.

- Доменные учетные записи пользователей (domain user accounts) определены в Active Directory. Благодаря однократному вводу пароля, такие учетные записи могут обращаться к ресурсам во всем домене. Они создаются в

оснастке Active Directory Users And Computers (Active Directory — пользователи и компьютеры).

- Локальные учетные записи пользователей (local user accounts) определены на локальном компьютере, имеют доступ только к локальному компьютеру и должны аутентифицировать себя, прежде чем смогут получить доступ к сетевым ресурсам. Локальные учетные записи пользователей создают в оснастке Local Users And Groups (Локальные пользователи и группы).

Примечание Только рядовые серверы и рабочие станции хранят локальные учетные записи пользователей и групп. На первом контроллере домена они перемещаются из локального диспетчера безопасности в Active Directory и преобразуются в доменные учетные записи.

Имена для входа в систему, пароли и открытые **сертификаты**

Все учетные записи пользователей распознаются по имени для входа в систему. В Windows 2000 это имя состоит из двух частей:

- имя пользователя — текстовая метка учетной записи;
- **домен пользователя или рабочая** группа — рабочая группа или домен, где находится пользователь.

Для пользователя WRSTANEK, чья учетная запись создана в домене MICROSOFT.COM, полное имя для входа в Windows 2000 — wrstanek@microsoft.com. Имя для предыдущих версий Windows — MICROSOFT\wrstanek.

При работе с Active Directory вам также может понадобиться указать полное доменное имя пользователя. Полное доменное имя группы — это сочетание DNS-имени домена, местоположения контейнера или ОП и имени группы. У пользователя Microsoft.com\Users\wrstanek, Microsoft.com — DNS-имя домена, Users — местоположение контейнера или ОП, а wrstanek — имя пользователя.

Учетные записи пользователей могут обладать связанными паролями и открытыми сертификатами. Пароли — это строки аутентификации для учетной записи. Открытые сертификаты сочетают открытый и закрытый ключ для идентификации пользователя. Вход в систему по паролю проходит интерактивно, При входе в систему с открытым сертификатом используются смарт-карта и считывающее устройство.

Идентификаторы безопасности и учетные записи пользователей

Хотя Windows 2000 отображает имена пользователей, чтобы описать привилегии и разрешения, ключевые идентификаторы учетных записей - - идентификаторы безопасности (security identifier, SID). SID — уникальные идентификаторы, генерируемые при создании учетных записей. SID состоит из префикса идентификатора безопасности домена и уникального относительного идентификатора, который был выделен хозяином относительных идентификаторов.

С помощью SID Windows 2000 отслеживает учетные записи независимо от имен пользователей. Два важнейших назначения SID: удобство изменения имен пользователей и возможность удаления учетных записей, не беспокоясь, что кто-то получит доступ к ресурсам, создав учетную запись с тем же именем.

Когда вы меняете имя пользователя, Windows 2000 сопоставляет прежний SID новому имени. Когда вы удаляете учетную запись, Windows 2000 считает, что конкретный SID больше недействителен. Если вы затем создадите учетную запись с тем же именем, она не будет иметь привилегий предыдущей записи, так как у нее будет иной SID.

Группы

Кроме учетных записей пользователя, в Windows 2000 есть группы. Группы позволяют предоставить разрешения схожим типам пользователей и упростить администрирование учетных записей. Если пользователь — член группы, которая вправе обращаться к ресурсу, то он тоже может к нему обратиться. Поэтому вы можете предоставить пользователю доступ к нужным ресурсам, просто включии его в подходящую группу. Хотя вы входите в систему под учетной записью пользователя, пойти в нее под учетной записью группы нельзя.

Поскольку в разных доменах Active Directory могут быть группы с одинаковыми именами, на группы часто ссылаются по полному имени -- *домен\имя_группы*, например, WORK\GMarketing соответствует группе GMarketing в домене WORK. При работе с Active Directory иногда нужно указывать полное доменное имя для группы — сочетание DNS-имени домена, имени контейнера или ОП и имени группы. *В* имени группы Microsoft.com\Users\Gmarketing, Micro-

soft.com — DNS-имя домена, Users — местоположение контейнера или ОП, а GMarketing — имя группы.

Примечание Служащим отдела маркетинга скорее всего понадобится доступ ко всем ресурсам, связанным с маркетингом. Вместо того чтобы открывать доступ к ним индивидуально, можно объединить пользователей в группу. Если позже пользователь перейдет в другой отдел, вы просто исключите его из группы, и все разрешения доступа будут отозваны.

Типы групп

В Windows 2000 три типа групп:

- **локальные группы** определяются и используются только на локальном компьютере, создаются в оснастке Local Users And Groups (Локальные пользователи и группы);
- группы **безопасности** обладают дескрипторами защиты, определяются в доменах в оснастке Active Directory Users And Computers (Active Directory — пользователи и компьютеры);
- группы **распространения** используются как списки рассылки электронной почты, не имеют дескрипторов безопасности и определяются в доменах в оснастке Active Directory Users And Computers.

Область действия группы

У групп могут быть разные области действия — *локальная доменная* (domain local), *встроенная локальная* (built-in local), *глобальная* (global) и *универсальная* (universal). От этого зависит, в какой части сети они действительны.

- **Локальные доменные группы** позволяют предоставить разрешения в одном домене. В состав локальных доменных групп входят лишь учетные записи (и пользователей, и компьютеров) и группы из домена, в котором они определены.
- **Встроенные локальные группы** обладают особыми разрешениями в локальном домене, и для простоты их часто называют *локальными доменными группами* (domain local groups). В отличие от других групп встроенные локальные нельзя создать или удалить — можно лишь изменить их состав. Ссылки на локальные доменные группы применяются к встроенным локальным группам, если не указано обратное.

- **Глобальные группы** обладают разрешениями для объектов в любом домене дерева или леса. В глобальную группу входят только учетные записи и группы из домена, в котором они определены.
- **Универсальные группы** имеют разрешения по всему дереву или лесу; в них входят учетные записи и группы из любого домена в дереве или лесу.

Примечание Универсальные группы очень полезны на больших предприятиях, где есть несколько доменов. Состав универсальных групп не должен часто меняться, так как любое изменение надо реплицировать во все глобальные каталоги (ГК) в дереве или лесу. Чтобы уменьшить количество изменений, включайте в универсальную группу только группы, а не сами учетные записи. Подробнее см. раздел «Когда использовать локальные доменные, глобальные и универсальные группы».

От области действия группы зависит, что вы можете делать с группой (табл. 7-1). О создании групп см. главу 8.

Табл. 7-1. Влияние области действия группы на ее характеристики.

Возможности	Локальная доменная область	Глобальная область	Универсальная область
Состав в основном режиме	Учетные записи, глобальные и универсальные группы из любого домена, локальные доменные только из того же домена.	Учетные записи и глобальные группы только из того же домена.	Учетные записи и группы из любого домена независимо от области действия.
Состав в смешанном режиме	Учетные записи и глобальные группы из любого домена.	Учетные записи только из того же домена.	Нельзя создать в домене смешанного режима.
Участник других групп	Можно поместить в другие локальные доменные группы и назначить разрешения только в том же домене.	Можно поместить в другие группы и назначить разрешения в любом домене.	Можно поместить в другие группы и назначить разрешения в любом домене.

Табл. 7-1. *(продолжение)*

Возможности	Локальная доменная область	Глобальная область	Универсальная область
Участник других групп	Можно поместить в другие локальные доменные группы и назначить разрешения только в том же домене.	Можно поместить в другие группы и назначить разрешения в любом домене.	Можно поместить в другие группы и назначить разрешения в любом домене.
Смена области действия	Можно преобразовать в универсальную область, если в их составе нет групп с локальной доменной областью.	Можно преобразовать в универсальную область, если они не являются участниками другой группы с глобальной областью.	Нельзя преобразовать ни в какую другую область.

Идентификаторы безопасности и учетные записи групп

Как и для учетных записей пользователей, Windows 2000 применяет уникальные идентификаторы безопасности (SID) для отслеживания учетных записей групп. Эта значит, что нельзя удалить учетную запись группы, а затем создать группу с тем же именем, чтобы у нее появились прежние разрешения и привилегии. У новой группы будет новый SID, и все разрешения и привилегии старой группы будут утеряны.

Windows 2000 создает маркер безопасности для каждого сеанса пользователя в системе. Он содержит идентификатор учетной записи пользователя и SID всех групп безопасности, к которым относится пользователь. Размер маркера растет по мере того, как пользователь добавляется в новые группы безопасности. Это влечет следующее.

- Чтобы пользователь вошел в систему, маркербезопасности должен быть передан процессу входа в систему. Поэтому по мере увеличения членства пользователя в группах безопасности процесс входа требует все больше времени.
- Чтобы выяснить разрешения доступа, маркер безопасности пересылается на каждый компьютер, к которому об-

ращается пользователь. Поэтому чем больше маркер безопасности, тем выше сетевой трафик.

Примечание Сведения о членстве в группах распространения не передаются в маркере безопасности, поэтому состав этих групп не влияет на размер маркера.

Когда использовать локальные доменные, глобальные и универсальные группы

Локальные доменные, глобальные и универсальные группы предоставляют множество параметров для конфигурирования групп в масштабе предприятия. В идеале следует использовать области групп для создания иерархий, схожих со структурой вашей организации и обязанностями групп пользователей.

- Локальные доменные группы обладают наименьшей сферой влияния и хорошо подходят для управления доступом к таким ресурсам, как принтеры и общие папки.
- Глобальные группы оптимальны для управления учетными записями пользователей и компьютеров в отдельном домене. Предоставляйте разрешения доступа к ресурсу, включая глобальную группу в локальную доменную.
- Универсальные группы обладают самой широкой сферой влияния. Используйте их для централизации групп, определенных в нескольких доменах. Обычно для этого в универсальную группу добавляется глобальная. Тогда при изменении состава глобальных групп изменения пе будут реплицироваться во все ГК, поскольку формально состав универсальных групп не меняется.

Примечание Если в вашей организации всего один домен, универсальные группы не нужны: стройте структуру групп на локальных доменных и глобальных. Если вы затем добавите другой домен в дерево или лес, вы легко расширите иерархию, чтобы она соответствовала новому состоянию сети.

Рассмотрим сценарий. Пусть у вас есть представительства в Сиэтле, Чикаго и Нью-Йорке. У каждого офиса собственный домен, являющийся частью одного дерева или леса: SEATTLE, CHICAGO и NY. Вы хотите упростить для администраторов (из любого офиса) управление сетевыми ресурсами, поэтому создаете идентичную структуру групп. В компании есть отделы маркетинга, И'Г и инженерный, но мы рассмотрим

лишь структуру отдела маркетинга. В каждом представительстве сотрудникам этого отдела нужен доступ к общему принтеру MarketingPrinter и общей папке MarketingData. Вам нужно, чтобы сотрудники могли совместно использовать и печатать документы. Скажем, Бобу из Сиэтла нужно печатать документы для Ральфа в Нью-Йорке, поэтому Бобу нужен доступ к квартальному отчету в общей папке в нью-йоркском офисе.

Сконфигурируем группы для отделов маркетинга в трех офисах.

1. Начнем с создания глобальных групп для каждой маркетинговой группы. В домене SEATTLE создадим группу GMarketing и добавим в нее сотрудников отдела маркетинга из Сиэтла. В домене CHICAGO создадим группу с тем же именем и добавим в нее сотрудников отдела маркетинга из Чикаго. В домене NY сделаем то же самое.
2. В каждом представительстве создадим локальные доменные группы, предоставив им доступ к общим принтерам и папкам. Назовем группу с доступом к принтеру LocalMarketingPrinter, а общую папку в домене Нью-Йорка - LocalMarketingData. Домены SEATTLE, CHICAGO и NY должны обладать собственными локальными группами.
3. Создадим универсальную группу UMarketing в домене каждого представительства. Добавим в нее группы SEATTLE\GMarketing, CHICAGO\GMarketing и NY\GMarketing.
4. Добавим UMarketing в группы LocalMarketingPrinter и LocalMarketingData в каждом представительстве. Сотрудники отдела маркетинга теперь смогут совместно использовать данные и принтеры.

Стандартные учетные записи пользователей и группы

При установке Windows 2000 создаются стандартные учетные записи пользователей и группы. Они предназначены для начальной настройки, необходимой для развития сети. Вот три типа стандартных учетных записей:

- **предопределенные** учетные записи пользователей и групп устанавливаются вместе с ОС;

- **встроенные** учетные записи пользователей и групп устанавливаются вместе с ОС, приложениями и службами;
- неявные — специальные группы, создаваемые неявно при обращении к сетевым ресурсам; их также называют *специальными идентификаторами* (special identities).

Примечание Хотя вы можете изменять параметры стандартных пользователей и групп, нельзя удалить пользователей и группы, созданные ОС, поскольку их нельзя воссоздать. SID старой и новой учетных записей не будут совпадать, и разрешения и привилегии этих записей будут утеряны.

Встроенные учетные записи пользователей

У встроенных учетных записей пользователя в Windows 2000 есть особое применение. Хотя все системы Windows 2000 обладают встроенной учетной записью LocalSystem, могут быть доступны и другие встроенные записи пользователей.

Учетная запись LocalSystem

Это мнимая учетная запись для выполнения системных процессов и обработки задач системного уровня, доступная только на локальной системе. Вы не можете менять параметры учетной записи LocalSystem средствами администрирования, равно как и входить под ней в систему.

Примечание Хотя пользователям нельзя войти в систему как LocalSystem, определенные процессы *могут* это делать. Например, службы Windows 2000 можно настроить на вход с учетной записью System (см. также главу 3).

Другие встроенные учетные записи

Когда вы устанавливаете дополнения или другие приложения на рабочей станции или сервере, можно установить и другие учетные записи по умолчанию. Обычно их можно потом удалить.

При установке информационных служб Интернета (Internet Information Services, IIS), вы обнаружите новые учетные записи: IUSR_*узел* и IWAM_*узел*,где *узел* — имя компьютера. IUSR_*узел* — встроенная учетная запись для анонимного доступа к IIS, а IWAM_*узел*служит IIS для запуска прикладных процессов. Эти учетные записи определяются в

Active Directory, когда они настроены в домене. Но они определяются как локальные пользователи, когда настроены па изолированном сервере или рабочей станции. Еще одна учетная запись, которую вы можете увидеть, — TSInternetUser — требуется службам терминала.

Предопределенные учетные записи пользователей

Вместе с Windows 2000 устанавливаются две записи: Administrator (Администратор) и Guest (Гость). На рабочих станциях и рядовых серверах, предопределенные учетные записи являются локальными для той системы, где они установлены.

У предопределенных учетных записей есть аналоги в Active Directory, которые имеют доступ по всему домену и совершенно независимы от локальных учетных записей на отдельных системах.

Учетная запись Administrator

Эта предопределенная учетная запись обладает полным доступом к файлам, каталогам, службам и другим ресурсам; ее нельзя отключить или удалить. В Active Directory она обладает доступом и привилегиями во всем домене. В остальных случаях Administrator обычно имеет доступ только к локальной системе. Хотя файлы и каталоги можно временно защитить от Administrator, эта запись всегда может получить контроль над любыми ресурсами, сменив разрешения доступа.

Совет Чтобы предотвратить несанкционированный доступ к системе или домену, убедитесь, что у этой записи надежный пароль. Кроме того, поскольку это известная учетная запись Windows 2000, переименуйте ее.

Обычно не требуется менять основные параметры учетной записи Administrator, однако иногда следует сменить такие дополнительные параметры, как членство в некоторых группах. По умолчанию Administrator домена — участник групп Administrators (Администраторы), Domain Admins (Администраторы домена), Domain Users (Пользователи домена), Enterprise Admins (Администраторы предприятия), Schema Admins (Администраторы схемы) и Group Policy Creator Owners (Создатели-владельцы групповой политики). Подробнее об этих группах см. следующий раздел.

Примечание В сети с доменами локальная учетная запись Administrator применяется в основном для управления системой сразу после установки. Это позволяет вам настраивать ОС, не опасаясь блокировки. Вероятно, вы не станете применять ее впоследствии — вместо этого включите ваших администраторов в группу Administrators. Это гарантирует, что вы сможете отозвать привилегии администраторов без изменения паролей для всех учетных записей Administrator.

В системе, которая является частью рабочей группы, где каждый компьютер управляется независимо от других, эта запись часто требуется для выполнения административных задач. При этом не следует настраивать индивидуальные учетные записи для каждого лица, обладающего административным доступом к системе. Лучше используйте одну учетную запись Administrator на каждом компьютере.

Учетная запись Guest

Предназначена для пользователей, которым нужен разовый или редкий доступ. Хотя гости обладают ограниченными системными привилегиями, будьте осторожны, применяя эту запись, поскольку она потенциально снижает безопасность. Поэтому запись Guest изначально отключена при установке Windows 2000.

Совет Решив задействовать запись Guest, убедитесь, что она наделена ограниченными правами, и регулярно меняйте для нее пароль. Как и с учетной записью Administrator, для предосторожности переименуйте запись Guest.

Встроенные группы

Встроенные группы устанавливаются со всеми рабочими станциями и серверами Windows 2000. Чтобы предоставить пользователю привилегии и разрешения встроенной группы, добавьте его в группу. Например, чтобы дать пользователю административный доступ к системе, включите его в локальную группу Administrators. Чтобы дать пользователю административный доступ к домену, включите его в локальную доменную группу Administrators в Active Directory.

Доступность определенных встроенных групп зависит от конфигурации системы (табл. 7-2).

Табл. 7-2. Доступность встроенных групп в зависимости от типа сетевого ресурса.

Имя группы	Тип группы	Домен Active Directory	Windows 2000 Professional или рядовой сервер
Account Operators (Операторы учета)	Встроенная локальная	Да	Нет
Administrators (Администраторы)	Встроенная локальная, локальная	Да	Да
Backup Operators (Операторы архива)	Встроенная локальная, локальная	Да	Да
Guests (Гости)	Встроенная локальная, локальная	Да	Да
Power Users (Опытные пользователи)	Локальная	Нет	Да
Pre-Windows 2000 Compatible Access (Пред-Windows 2000 доступ)	Встроенная локальная	Да	Нет
Print Operators (Операторы печати)	Встроенная локальная	Да	Нет
Replicator (Репликатор)	Встроенная локальная, локальная	Да	Да
Server Operators (Операторы сервера)	Встроенная локальная	Да	Нет
Users (Пользователи)	Встроенная локальная, локальная	Да	Да

Предопределенные группы

Предопределенные группы устанавливаются с доменами Active Directory и служат для назначения пользователям дополнительных разрешений. Предопределенные группы включают в себя локальные доменные, глобальные и универсальные группы. Доступность конкретных предопределенных групп зависит от конфигурации домена (табл. 7-3).

Примечание Область действия групп Enterprise Admins и Schema Admins может быть универсальной либо глобальной в зависимости от рабочего режима домена: в смешанном они глобальные, а в основном — универсальные.

Табл. 7-3. Доступность предопределенных групп в зависимости от конфигурации домена.

Имя группы	Тип группы	Устанавливается
Cert Publishers	Глобальная	По умолчанию
DHCP Administrators (Администраторы DHCP)	Локальная доменная	Вместе с DHCP
DHCP Users (Пользователи DHCP)	Локальная доменная	Вместе с DHCP
DnsAdmins	Локальная доменная	Вместе с DNS
DnsUpdateProxy	Глобальная	Вместе с DNS
Domain Admins (Администраторы домена)	Глобальная	По умолчанию
Domain Computers (Компьютеры домена)	Глобальная	По умолчанию
Domain Controllers (Контроллеры домена)	Глобальная	По умолчанию
Domain Guests (Гости домена)	Глобальная	По умолчанию
Domain Users (Пользователи домена)	Глобальная	По умолчанию
Enterprise Admins	Универсальная/ глобальная	По умолчанию
Group Policy Creator Owners (Создатели-владельцы групповой политики)	Глобальная	По умолчанию
RAS and IAS Servers (Серверы RAS и IAS)	Локальная доменная	Вместе со службами удаленного доступа
Schema Admins (Администраторы схемы)	Универсальная/ глобальная	По умолчанию
WINS Users (Пользователи WINS)	Локальная доменная	Вместе с WINS

Неявные группы и специальные идентификаторы

В Windows NT неявные группы назначались неявно при входе в систему, исходя из того, как пользователь обращался к сетевому ресурсу. Так, если он обращался к ресурсу через интерактивный вход, то автоматически становился участником неявной группы Interactive. Б Windows 2000 объектный подход к структуре каталога изменил первоначальные пра-

вила для неявных групп. Хотя по-прежнему нельзя просмотреть состав неявных системных групп, вы вправе включать в них пользователей, группы и компьютеры.

Состав специальной встроенной группы может варьироваться неявно, например при входе в систему, или явно — через разрешения доступа. Как и для других стандартных групп, доступность неявных групп зависит от конфигурации (табл. 7-4).

Табл. 7-4. Доступность неявных групп в зависимости от типа сетевого ресурса.

Имя группы	Домен Active Directory	Windows 2000 Professional или рядовой сервер
Anonymous Logon (Анонимный вход)	Да	Да
Authenticated Users (Прошедшие проверку)	Да	Да
Batch (Пакетное задание)	Да	Да
Creator Group (Создатель группы)	Да	Да
Creator Owner (Создатель-владелец)	Да	Да
Dialup (Удаленный доступ)	Да	Да
Enterprise Domain Controllers (Контроллеры домена предприятия)	Да	Нет
Everyone (Все)	Да	Да
Interactive (Интерактивные)	Да	Да
Network (Сеть)	Да	Да
Proxy (Прокси)	Да	Нет
Restricted (Ограниченные)	Да	Нет
Self	Да	Нет
Service (Служба)	Да	Да
System (Система)	Да	Да
Terminal Server User (Пользователь служб терминалов)	Нет	Да

Возможности учетных записей

Чтобы назначить пользователю те или иные права, добавьте его в группы, а чтобы лишить — удалите из соответствующих групп. В Windows 2000 учетной записи можно назначить следующие типы прав.

- **Привилегия** позволяет выполнять определенную административную задачу, например отключать систему. Можно назначать привилегии как пользователям, так и группам.
- **Права на вход в систему** предоставляют разрешения на вход в систему, например локально. Можно назначить права на вход и пользователям, и группам.
- **Встроенные возможности** назначаются группам и содержит их автоматические возможности. Встроенные возможности предопределены и неизменны, но их можно делегировать пользователям с разрешением управлять объектами, ОП или другими контейнерами. Так, способность создавать, удалять и управлять учетными записями пользователей дается администраторам и операторам учета. Член группы Administrators может создавать, удалять и управлять учетными записями пользователей.
- **Разрешения доступа** определяют, какие действия можно выполнять над сетевыми ресурсами, например возможность создать файл в каталоге. Можно назначать разрешения доступа пользователям, компьютерам и группам (см. также главу 13).

Хотя вы не вправе менять встроенные возможности группы, вы можете изменить ее стандартные права. Так, администратор может отменить сетевой доступ к компьютеру, удалив право группы на доступ к этому компьютеру из сети.

Привилегии

Привилегии назначаются через групповые политики, применяемые к отдельным компьютерам, ОП и доменам. Хотя привилегии можно назначать и пользователям, и группам, их обычно назначают группам. Так, пользователям автоматически назначаются соответствующие привилегии, когда они становятся членами группы. Назначение привилегий группам упрощает управление учетными записями пользователей.

Ниже кратко описаны привилегии, назначаемые пользователям и группам (табл. 7-5) (см. также главу 8).

Табл. 7-5. Привилегии Windows 2000 для пользователей и групп.

Привилегия	Описание
Act as part of the operating system (Работа в режиме операционной системы)	Позволяет процессу аутентифицироваться как любому пользователю и получать доступ к ресурсам как любому пользователю. Процессы, которым требуется эта привилегия, должны использовать учетную запись LocalSystem, у которой уже есть эта привилегия.
Add workstations to domain (Добавление рабочих станций к домену)	Позволяет пользователям добавлять компьютеры в домен.
Back up files and directories (Архивирование файлов и каталогов)	Позволяет пользователям архивировать систему независимо от разрешений, заданных для файлов и каталогов.
Bypass traverse checking (Обход перекрестной проверки)	Позволяет пользователям проходить через каталоги при навигации но пути объекта независимо от разрешений, заданных для каталогов; не позволяет пользователям просматривать содержимое каталога.
Change the system time (Изменение системного времени)	Позволяет пользователям задавать время на системных часах.
Create *я* pagefile (Создание страничного файла)	Позволяет пользователям создавать и изменять размер страничного файла для виртуальной памяти.
Create a token object (Создание маркерного объекта)	Позволяет процессам создавать объекты-маркеры, через которые можно получять доступ к локальным ресурсам. Процессы, которым требуется эта привилегия, должны использовать учетную запись LocalSystem, у которой уже есть эта привилегия.
Create permanent shared objects (Создание постоянных объектов совместного использования)	Позволяет процессам создавать объекты каталога в диспетчере объектов Windows 2000. У большинства компонентов уже есть эта привилегия, и нет необходимости специально назначать ее.
Debug programs (Отладка программ)	Позволяет пользователям выполнять отладку.

Табл. 7-5. *(продолжение)*

Привилегия	Описание
Enable user and computer accounts to be trusted for delegation (Разрешение доверия к учетным записям при делегировании)	Разрешает пользователям или компьютерам изменять или применять параметр Trusted For Delegation при условии, что у них есть право на запись объекта.
Force shutdown of a remote system (Принудительное удаленное завершение)	Разрешает пользователям выключать компьютер из удаленной точки в сети.
Generate security audits (Создание журналов безопасности)	Позволяет процессам записывать в журнал безопасности для аудита доступа к объектам.
Increase quotas (Увеличение квот)	Позволяет процессам повышать квоты процессора, назначенные другому процессу, при условии, что у них есть право на запись для процесса.
Increase scheduling priority (Увеличение приоритета диспетчирования)	Разрешает процессам повышать приоритет, назначенный другим процессам при условии, что у них есть право на запись для процесса.
Load and unload device drivers (Загрузка и выгрузка драйверов устройства)	Позволяет пользователям устанавливать и удалять драйверы устройств Plug and Play. Не влияет на драйверы остальных устройств, которые могут быть установлены только администраторами.
Lock pages in memory (Закрепление страниц в памяти)	В Windows NT позволяет процессам хранить данные в физической памяти, запрещая системе выгружать страницы данных в виртуальную память на диске. В Windows 2000 не используется.
Manage auditing and security log (Управление аудитом и журналом безопасности)	Позволяет пользователям задавать параметры аудита и просматривать журнал безопасности (сначала нужно включить аудит в групповой политике).
Modify firmware environment values (Изменение параметров среды оборудования)	Разрешает пользователям и процессам изменять переменные системной среды.
Profile a single process (Профилирование одного процесса)	Разрешает пользователям контролировать быстродействие несистемных процессов.

Табл. 7-5. *(продолжение)*

Привилегия	Описание
Profile system performance (Профилирование загруженности системы)	Разрешает пользователям контролировать быстродействие системных процессов.
Remove computer from docking station (Извлечение компьютера из стыковочного узла)	Позволяет пользователям извлечь переносной компьютер из стыковочной станции.
Replace a process-level token (Замена маркера уровня процесса)	Позволяет процессам перемещать метку по умолчанию для второстепенных процессов.
Restore files and directories (Восстановление файлов и каталогов)	Разрешает пользователям восстанавливать из архива файлы и каталоги независимо от разрешений, заданных для файлов и каталогов.
Shut down the system (Завершение работы системы)	Разрешает пользователям выключать локальный компьютер.
Synchronize directory service data (Синхронизация данных службы каталогов)	Разрешает пользователям синхронизировать данные службы каталогов на контроллерах доменов.
Take ownership of files Or Other Objects (Овладение файлами или иными объектами)	Разрешает пользователям завладевать любыми объектами Active Directory.

Права на вход в систему

Право на вход в систему — тип права пользователя, который предоставляет разрешения для входа в систему. Вы можете назначать права на вход в систему и пользователям, и группам. Как и с привилегиями, права на вход в систему назначаются через групповые политики; назначайте их группам, а не пользователям.

Ниже описаны права на вход в систему, которые можно назначить пользователям и группам, (табл. 7-6) (см. также главу 8).

Табл. 7-6. Права на вход в систему для пользователей и групп.

Право на вход в систему	Описание
Access this computer from the network (Доступ к компьютеру из сети)	Разрешает пользователям связываться с компьютером по сети. По умолчанию предоставляется группам Administrators, Everyone и Power Users.
Deny access to this computer from the network (Отказ в доступе к компьютеру из сети)	Запрещает доступ к этому компьютеру.
Deny logon as batch job (Отказ во входе в качестве пакетного задания)	Отказывает в праве на вход в систему через пакетное задание или сценарий.
Deny logon as service (Отказать во входе в качестве службы)	Отказывает в праве на вход в систему службе.
Deny logon locally (Отклонить локальный вход)	Отказывает в праве на вход в систему с клавиатуры компьютера.
Log on as a batch job (Вход в качестве пакетного задания)	Позволяет пользователям входить в систему через пакетную очередь. Не поддерживается в текущем выпуске Windows 2000. По умолчанию эта привилегия предоставлена группе Administrators.
Log on as a service (Вход в качестве службы)	Разрешает участникам безопасности входить в систему как служба (как вариант установления контекста безопасности). Учетная запись LocalSystem всегда сохраняет за собой право на вход в систему как служба. Любые службы, выполняющиеся под отдельными учетными записями, должны обладать этим правом. По умолчанию не предоставляется всем службам.
Log on locally (Локальный вход в систему)	Позволяет пользователям войти в систему с клавиатуры компьютера. По умолчанию предоставляется группам Administrators, Account Operators, Backup Operators, Print Operators и Server Operators.

Встроенные возможности групп в Active Directory

Б следующих двух таблицах описаны самые распространенные возможности, назначаемые по умолчанию. В табл. 7-7

перечислены стандартные права для групп в доменах Active Directory, в том числе привилегии и права на вход в систему. Учтите, любое действие, доступное группе Everyone, доступно все группам, включая Guests (Гости), т. е. хотя у группы Guests нет явного разрешения на обращение к компьютеру из сети, Guests сможет получить доступ к системе, так как группа Everyone имеет это право.

Табл. 7-7. Стандартные **права** пользователей для групп **в Active** Directory.

Право пользователя	Назначено группам
Access this computer from the network	**Everyone**
Add workstations to domain	Administrators
Back up files and directories Backup Operators	Administrators, Server Operators,
Bypass traverse checking	Everyone
Change the system time	Administrators, Server Operators
Create a pagefile	Administrators
Debug programs	Administrators
Force shutdown from a remote system	Administrators, Server Operators
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Log on locally	Administrators. Server Operators, Account Operators, Backup Operators, Print Operators
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile a single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Administrators
Restore files and directories	Administrators, Server Operators, Backup Operators
Shut down the system	Administrators. Server Operators, Account Operators. Backup Operators, Print Operators
Take ownership of files or other objects	Administrators

В табл. 7-8 перечислены стандартные права для локальных групп на рядовых серверах и рабочих станциях; здесь также приведены и привилегии, и права на вход. Учтите, что на этих системах группа Power Users обладает привилегиями, которых нет у обычных пользователей.

Табл. 7-8. Стандартные права пользователей для локальных групп.

Право пользователя	Назначено группам
Access this computer from the network	Administrators, Power Users, Everyone
Back up files and directories	Administrators, Backup Operators
Bypass traverse checking	Everyone
Change the system time	Administrators, Power Users
Create a pagefile	Administrators
Debug programs	Administrators
Force shutdown from a remote system	Administrators
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Log on locally	Administrators, Backup Operators. Power Users, Users, Everyone, Guests
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile a single process	Administrators, Power Users
Profile system performance	Administrators
Remove computer from docking station	Administrators, Power Users, Users
Restore files and directories	Administrators, Backup Operators
Shut down the system	Administrators, Backup Operators, Power Users, Users
Take ownership of files or other objects	Administrators

В табл. 7-9 перечислены возможности, которые можно делегировать другим пользователям и группам. Заметьте: в числе записей с ограниченным доступом запись Administrator, учетные записи администраторов и учетные записи групп

Administrators, Server Operators, Account Operators, Backup Operators и Print Operators. Поэтому группа Account Operators не может создавать или изменять их.

Табл. 7-9. Другие возможности встроенных **и локальных групп.**

Задача	Разрешает пользователям	Обычно назначается группам
Assign user rights (Назначение прав пользователей)	Назначать права для других пользователей	Administrators
Create, delete, and manage user accounts (Создание, удаление и управление учетными записями пользователей)	Администрировать доменные учетные записи пользователей	Administrators, Account Operators
Modify the membership of a group (Изменение членства в группе)	Добавлять и удалять пользователей из доменных групп	Administrators, Account Operators
Create and delete groups (Создание и удаление групп)	Создавать/удалять группы	Administrators, Account Operators
Reset passwords on user accounts (Смена паролей для пользователей)	Сбрасывать пароли учетных записей	Administrators. Account Operators
Read all user information (Чтение всей информации пользователя)	Просматривать информацию учетной записи пользователя	Administrators, Server Operators, Account Operators
Manage group policy links (Управление связями групповой политики)	Применять существующие групповые политики к сайтам, доменам и ОП, для которых у них есть право на запись соответствующих объектов	Administrators
Manage printers (Управление принтерами)	Настраивать принтер и управлять очередями печати	Administrators, Server Operators, Printer Operators
Create and delete printers (Создание и удаление принтеров)	Создавать/удалять принтеры	Administrators, Server Operators, Printer Operators

Стандартные учетные записи групп

Стандартные группы спроектированы универсальными. Если назначить пользователей в правильные группы, управлять рабочими группами или доменами Windows 2000 будет гораздо легче. Однако в таком разнообразии групп понять назначение каждой из них не просто. Для этого поделим группы на пять категорий: группы администраторов, операторов, пользователей, компьютеров и неявные группы.

Группы администраторов

Администратор обладает широким доступом к сетевым ресурсам. Администраторы могут создавать учетные записи, изменять права пользователя, устанавливать принтеры, управлять общими ресурсами и т. п. Основные группы администраторов; Administrators, Domain Admins и Enterprise Admins (табл. 7-10).

Примечание Локальный пользователь Administrator и глобальные группы Domain Admins и Enterprise Admins являются членами группы Administrators. Членство в Administrator необходимо для доступа к локальному компьютеру, Членство в группе Domain Admins позволяет другим администраторам обращаться к системе из любой точки домена. Членство в Enterprise Admins позволяет другим администраторам обращаться к системе из других доменов в том же дереве или лесу. Чтобы предотвратить широкий административный доступ к домену из любой точки предприятия, удалите Enterprise Admins из этой группы.

Табл. 7-10. Обзор групп администраторов.

Тип группы администраторов	Сетевая среда	Область действия группы	Участники	Администрирование учетной записи группы
Administrators	Домены Active Directory	Локальная доменная	Administrator, группы Domain Admins, Enterprise Admins	Группа Administrators
Administrators	Рабочие станции, компьютеры вне домена	Локальная	Administrator	Группа Administrators

Табл. 7-10. *(продолжение)*

Тип группы администраторов	Сетевая среда	Область действия группы	Участники	Администрирование учетной записи группы
Domain Admins	Домены Active Directory	Глобальная	Administrator	Группа Administrators
Enterprise Admins	Домены Active Directory	Глобальная или универсальная	Administrator	Группа Administrators

Administrators — локальная группа, предоставляющая полный административный доступ к отдельному компьютеру или одному домену в зависимости от ее расположения. Поскольку у этой учетной записи полный доступ, осторожно добавляйте пользователей в эту группу. Чтобы назначить кого-то администратором локального компьютера или домена, нужно лишь включить этого человека в данную группу. Только члены группы Administrators могут изменять эту учетную запись.

Глобальная группа Domain Admins призвана помочь в администрировании всех компьютеров в домене. У этой группы есть административный контроль над всеми компьютерами в домене, поскольку по умолчанию она входит в группу Administrators. Чтобы назначить кого-то администратором домена, добавьте его в эту группу.

Совет В домене Windows 2000 локальный пользователь Administrator по умолчанию является членом группы Domain Admins, т. е. если кто-то войдет на компьютер как администратор и этот компьютер является частью домена, то получит полный доступ ко всем ресурсам в домене. Чтобы избежать этого, удалите локальную учетную запись Administrator из группы Domain Admins.

Глобальная группа Enterprise Admins позволяет администрировать все компьютеры в дереве или лесу. Она имеет административный контроль над всеми компьютерами на предприятии, так как по умолчанию включена в группу Administrators. Чтобы назначить кого-то администратором предприятия, добавьте его в эту группу.

Совет В домене Windows 2000 локальный пользователь Administrator по умолчанию является членом группы Enter-

prise Admins, т. е. если кто-то войдет на компьютер как администратор и этот компьютер является частью домена, то получит полный доступ к дереву или лесу. Чтобы избежать этого, удалите локальную учетную запись Administrator из группы Enterprise Admins.

Группы операторов

Операторы — это пользователи, у которых есть привилегии на выполнение очень специфичных административных задач типа создания учетных записей или архивирования файловых систем. По умолчанию никакие учетные записи групп или пользователей не включены л группы операторов. Эта функциональность задумана, чтобы вы могли явно предоставлять доступ к этим учетным записям. Кроме того, поскольку эти группы — локальные, операторы могут выполнять задания только на определенном компьютере (табл. 7-11).

Account Operators — локальная группа, предоставляющая пользователю ограниченные привилегии по созданию учетной записи. Члены этой группы могут создавать и изменять большинство типов учетных записей, включая записи пользователей, локальных и глобальных групп. Они также могут локально входить на контроллеры домена. Впрочем, группа Account Operators не может управлять учетной записью пользователя Administrator, записями администраторов и групп Administrators, Server Operators. Account Operators, Backup Operators и Print Operators. Члены этой группы также не могут изменять права пользователя.

Табл. 7-11. Обзор групп операторов.

Тип группы операторов	Сетевая среда	Область действия группы	Участники	Администрирование учетной записи группы
Account Operators	Домены Active Directory	Встроенная локальная	Нет	Группа Administrators
Backup Operators	Любой сервер или рабочая станция	Встроенная локальная, Локальная	Нет	Группа Administrators
Print Operators	Домены Active Directory	Встроенная локальная	Нет	Группа Administrators
Server Operators	Домены Active Directory	Встроенная локальная	Нет	Группа Administrators

Табл. 7-11. Обзор групп операторов.

Тип группы операторов	Сетевая среда	Область действия группы	Участники	Администрирование учетной записи группы
Replicator	Любой сервер или рабочая станция	Встроенная локальная, локальная	Нет	Группы Administrators, Account Operators, Server Operators

Члены локальной группы Backup Operators могут архивировать и восстанавливать файлы/каталоги на рабочих станциях и серверах в домене Windows 2000. Они могут входить на компьютер, архивировать или восстанавливать файлы и завершать работу компьютера. В зависимости от настройки члены этой группы могут архивировать файлы независимо от того, есть ли у них право на чтение или запись этих файлов. Впрочем, они не могут менять разрешения доступа к файлам или выполнять другие административные задачи.

Print Operators — локальная группа для управления сетевыми принтерами. Ее члены могут управлять принтерами в домене Windows 2000. Они могут открывать доступ к принтерам и задавать связанные с ними привилегии. Члены группы Print Operators могут также локально входить на сервер и завершать его работу.

Члены локальной группы Server Operators могут выполнять основные задачи администратора, включая открытие доступа к ресурсам сервера, архивирование и восстановления файлов и т. п. Как и остальные записи операторов, Server Operators также вправе локально входить в сервер и завершить его работу. Члены этой группы могут выполнять типичные задачи администрирования сервера.

Специальная учетная запись Replicator используется со службой репликации каталога. Администраторы и операторы могут настраивать эту службу для управления репликацией файлов и каталогов в домене. Вы можете настроить специальную учетную запись пользователя для работы со службой репликации и добавить ее в эту группу.

Группы пользователей

Windows 2000 предоставляет несколько типов учетных записей пользователя согласно требованиям разных сетевых

сред: Users, Domain Users, Power Users, Guests и Domain Guests (табл. 7-12).

Табл. 7-12. Обзор групп пользователей.

Тип группы пользователей	Сетевая среда	Область действия группы	Члены	Администрирование учетной записи группы
Users	Домены Active Directory, рядовой сервер домена или рабочая станция	Встроенная локальная, локальная	Authenticated Users, Domain Users	Группы Administrators, Account Operators
Users	Изолированная рабочая станция или сервер	Локальная	Учетная запись пользователя, выбранная во время установки ОС	Группа Administrators
Domain Users	Домены Active Directory	Глобальная	Administrators, Guest	Группы Administrators, Account Operators
Power Users	Рядовой сервер домена или рабочая станция	Локальная	Interactive; учетная запись пользователя, выбранная во время установки ОС	Группа Administrators
Power Users	Изолированная рабочая станция или сервер	Локальная	Учетная запись пользователя, выбранная во время установки ОС	Группа Administrators
Guest	Домены Active Directory	Встроенная локальная	Domain Guests, Guest	Группы Administrators, Account Operators
Guest	Рядовой сервер домена или рабочая	Локальная	Guest	Группа Administrators

Табл. 7-12. *(продолжение)*

Тип группы пользователей	Сетевая среда	Область действия группы	Члены	Администрирование учетной записи группы
	станция; изолированная рабочая станция или сервер			
Domain Guest	Домены Active Directory	Глобальная	Guest	Группа Administrators, Account Operators

Пользователи выполняют большую часть своей работы на одной рабочей станции Windows 2000. Поэтому у членов группы Users больше ограничений, чем привилегий. По умолчанию они не могут локально войти на сервер Windows 2000, действующий как контроллер домена, но они могут обратиться к ресурсам контроллера через сеть.

На рабочих станциях Windows 2000 члены этой группы могут локально войти на рабочую станцию, сохранить локальный профиль, блокировать рабочую станцию и отключать ее, а также создать локальные группы и управлять ими.

В доменах Windows 2000 неявно аутентифицированные пользователи и глобальная группа Domain Users по умолчанию включены в эту группу. Для рабочих групп или изолированных рабочих станций нет предопределенных членов этой группы.

Domain Users — глобальная группа для пользователей в доменах Active Directory. Создаваемые пользователи домена автоматически добавляются в нее. По умолчанию локальные записи Administrator и Guest — члены этой группы.

Группа Power Users существует только на компьютерах, которые не являются контроллерами домена. Она обладает всеми привилегиями Users, а также некоторыми дополнительными, например, ее члены способны изменять параметры компьютера и устанавливать программы. Чтобы дать пользователям рабочих станций Windows 2000 дополнительный контроль, добавьте их в группу Power Users.

Гости — пользователи с весьма ограниченными привилегиями. Они могут удаленно обратиться к системе и ее ресур-

сам, но не вправе выполнять большинство остальных задач. В доменах Active Directory, членами этой группы являются группа Domain Guests и локальный пользователь Guest. На контроллерах вне домена единственный член — Guest.

Примечание Любое действие, доступное группе Everyone, доступно и группе Guests, т. е. член локальной группы Guests может выполнять любые задачи, которые разрешены пользователям из группы Everyone.

Члены группы Domain Guests являются пользователями с привилегиями гостя во всем домене. По умолчанию локальный пользователь Guest — член этой группы. Поэтому каждый раз, когда вы создаете локальную учетную запись гостя в домене Windows 2000, этот гость получает доступ ко всему домену.

Группы компьютеров

Windows 2000 предоставляет два типа учетных записей компьютеров, чтобы настраивать разрешения для рядовых серверов, рабочих станций и контроллеров домена: Domain Computers и Domain Controllers (табл, 7-13).

Табл. 7-13. Обзор групп компьютеров.

Тип группы компьютеров	Сетевая среда	Область действия группы	Члены	Администрирование учетной записи группы
Domain Computers	Домены Active Directory	Глобальная	Все рядовые серверы и рабочие станции в домене	Группы Administrators. Account Operators
Domain Controllers	Домены Active Directory	Глобальная	Все контроллеры домена	Группы Administrators, Account Operators

Группа Domain Computers служит для стандартной настройки разрешений для рядовых серверов и рабочих станций в домене. По умолчанию у Domain Computers больше ограничений, чем возможностей, что отражает их роль в среде домена.

Группа Domain Controllers служит для настройки разрешений для контроллеров домена. По умолчанию у Domain Controllers больше возможностей, чем ограничений, что отражает их высокоприоритетную роль в среде домена.

Встроенные системные группы

В Windows 2000 есть несколько встроенных системных групп, позволяющих назначить разрешения в конкретных ситуациях. Разрешения для таких групп обычно определяются неявно, но вы вправе назначать их самостоятельно, когда изменяете объекты Active Directory.

- **Anonymous Logon** (Анонимный вход) Любой пользователь обращающийся к системе через анонимный вход, обладает идентификатором Anonymous Logon. Он применяется для анонимного доступа к таким ресурсам, как Web-страницы на серверах предприятия.
- Authenticated **Users** (Прошедшие проверку) Любой пользователь, обращающийся к системе через процесс входа, включается в группу Authenticated Users. Эта группа применяется для разрешения доступа к общим ресурсам в домене, таким как файлы в общей панке, которые должны быть доступны всем сотрудникам организации.
- **Batch** (Пакетное задание) Любой пользователь или процесс, обращающийся к системе как пакетное задание (или через пакетную очередь), включается в эту группу. С ее помощью пакетные задания выполняются по расписанию,
- Creator **Group** (Создатель группы) Windows 2000 использует эту группу для автоматического предоставления разрешений доступа пользователям, которые являются членами той же группы (групп), что и создатель файла или каталога.
- **Creator Owner** (Создатель-владелец) Пользователь, создавший файл или каталог, является членом этой группы. Б Windows 2000 эта группа применяется для автоматического предоставления разрешений создателю файла или каталога.
- **Dial-Up** (Удаленный доступ) Каждый пользователь, обращающийся к системе через коммутируемое соединение, обладает идентификатором Dial-Up. Этот идентификатор помогает отличить таких пользователей от других.
- **Enterprise Domain Controllers** (Контроллеры домена предприятия) Контроллеры домена с ролями и обязательствами, действующими на всем предприятии, включаются в группу Enterprise Domain Controllers. Это по-

зволяет им выполнять определенные задачи на предприятии с использованием транзитивного доверия.

- Everyone (Все) Все интерактивные, сетевые, коммутируемые и прошедшие проверку пользователи — члены группы Everyone. Эта группа служит для предоставления широкого доступа к системным ресурсам.
- **Interactive** (Интерактивные) Каждый пользователь, вошедший в локальную систему, включается в группу Interactive. Она позволяет разрешить доступ к ресурсу *только локальным* пользователям.
- Network (Сеть) Каждый пользователь, обращающийся к системе через сеть, включается в эту. Она позволяет разрешить доступ к ресурсу *только удаленным* пользователям.
- **Proxy** (Прокси) Содержит пользователей и компьютеры, обращающихся к ресурсам через прокси-сервер (используется, когда в сети есть прокси-серверы).
- Restricted (Ограниченные) Содержит пользователей и компьютеры с ограниченным доступом. На рядовом сервере или рабочей станции в эту группу включается локальный пользователь из группы Users (но не группы Power Users).
- Self Содержит сам объект и позволяет ему изменять себя.
- Service (Служба) Представляет службы, обращающиеся к системе. Предоставляет доступ к процессам, выполняемым службами Windows 2000.
- System (Система) Сама ОС Windows 2000 состоит в этой группе; используется, когда ОС нужно выполнить функцию системного уровня.
- **Terminal Server User** (Пользователь служб терминалов) Каждый пользователь, обращающийся к системе через службы терминалов, состоит в группе Terminal Server User. Это позволяет пользователям сервера терминалов обращаться к приложениям сервера и выполнять другие задачи со службами терминала.

Глава 8

Создание учетных записей пользователей и групп

Основной частью работы администратора является создание учетных записей пользователей. Они позволяют Microsoft Windows 2000 управлять информацией о пользователях, включая полномочия и права доступа. Для этого служат:

- Active Directory Users And Computers (Active Directory — пользователи и компьютеры) — средство администрирования учетных записей в домене Active Directory;
- Local Users And Groups (Локальные пользователи и группы) — средство администрирования учетных записей на локальных компьютерах.

В этой главе описано создание учетных записей доменов, локальных пользователей и групп.

Настройка и формирование учетной записи пользователя

Прежде чем создавать учетные записи, вы должны определить политики, которые будете использовать при их настройке в рамках организации.

Политика именования учетных записей

Ключевая политика, которую нужно установить, — схема именования учетных записей. Учетная запись пользователя имеет *отображаемое (или полное) имя* (display name) и *имя для входа* (logon name). Первое отображается пользователю и упоминается в его сеансах. Второе применяется при входе в домен. Об именах для входа мы кратко говорили в главе 7.

Правила для отображаемых имен

В Windows 2000 отображаемое имя обычно является именем и фамилией пользователя, по вы можете назначить ему любое строковое значение. При этом:

- локальное отображаемое имя должно быть уникальным на рабочей станции;
- отображаемые имена должны быть уникальными во всем домене;
- отображаемые имена должны содержать не более 64 символов;
- отображаемые имена могут содержать буквенно-цифровые и специальные символы.

Правила имен для входа

Имена для входа даются по таким правилам.

- Локальные имена для входа должны быть уникальны на рабочей станции, а глобальные имена для входа — во всем домене.
- Имена для входа могут содержать до 104 символов, однако имена длиной более 64 символов неудобно использовать.
- Имя для входа, совместимое с Windows NT 4.0 или более ранней версией, дается всем учетным записям и по умолчанию соответствует первым 20 символам имени для входа в Windows 2000. Это имя должно быть уникальным во всем домене.
- Пользователи, входящие в домен с компьютеров Windows 2000, могут применять свои имена для входа как для Windows 2000, так и для Windows NT 4.0 или более ранней версии независимо от рабочего режима домена.
- Имена для входа не могут содержать символов:

  « \ \ [ ] : ; | = , + * ? < >

- Имена для входа могут содержать все другие специальные символы, включая пробелы, точки, тирс и символы подчеркивания. Но вообще использование пробелов в именах учетных записей не рекомендуется.

Примечание Хотя Windows 2000 хранит имена пользователей в том регистре, в котором вы их ввели, от регистра

они не зависят. Так, вы можете получить доступ к учетной записи Администратора, введя как «Администратор», так и «администратор». Имена пользователей хранят регистр, но не чувствительны к нему.

Схемы именования

В небольших организациях стремятся назначить имена для входа, применяя имя или фамилию пользователя. Но в организации любого размера может быть несколько Томов, Диков и Гарри. Поэтому вместо того, чтобы переделывать схему назначения имен для входа, лучше сразу все сделать по уму. Для назначения имени учетным записям применяйте согласованную процедуру, которая позволит расти вашей базе пользователей, ограничит конфликты имен и гарантирует, что у ваших учетных записей защищенные имена. Типы схем назначения имен могут быть следующими.

- **Имя и первая буква фамилии пользователя —** имя пользователя сочетается с первой буквой его фамилии. Для William Stanek используется *Williams* или *bills.* Эта схема непрактична для больших организаций.
- **Первая буква имени и фамилия пользователя —** первая буква имени пользователя сочетается с фамилией. Для William Stanek используется *wstanek.* Эта схема также непрактична для больших организаций.
- **Инициалы и фамилия пользователя —** сочетаются инициалы пользователя с его фамилией. Для имени William R. Stanek используется *wrstanek.*
- **Инициалы и первые пять букв фамилии пользователя —** сочетаются инициалы пользователя с первыми пятью буквами его фамилии. Для имени William R. Stanek используется *wrstane.*
- **Имя и фамилия пользователя** — вы сочетаете имя и фамилию пользователя. Для разделения имени и фамилии можно использовать символ подчеркивания (_) или дефис (-). Для William Stanek вы используете *william_stanek* или *william-stanek.*

Примечание В системах с повышенной безопасностью имени для входа можно назначить цифровой код длиной не менее 20 символов. Соединение такого метода назначения имен со смарт-картами и устройствами для их чтения по-

зволяет пользователям быстро войти в сеть. Не беспокойтесь, у пользователей по-прежнему будет **отображаемое имя,** удобное для чтения.

Пароли и учетные политики

Для аутентификации доступа к ресурсам сети учетные записи Windows 2000 используют пароли и открытые сертификаты.

Защитите пароли

Пароль — это чувствительная к регистру строка длиной до 104 символов для службы каталогов Active Directory и до 14 — для диспетчера безопасности Windows NT. В паролях можно применять буквы, цифры и знаки. Windows 2000 сохраняет пароль в зашифрованном виде в базе данных учетных записей.

Однако просто пароль не предотвратит несанкционированного доступа к сетевым ресурсам. Вы должны применять *защищенные* пароли: их труднее разгадать и взломать. Вы можете затруднить взлом паролей, комбинируя все возможные типы символов, включая буквы верхнего и нижнего регистров, цифры и знаки. Например, вместо строки happydays вы можете использовать в качестве пароля haPPy2Days&, Ha**y!dayS или даже h*PPY%d*ys.

К сожалению, не имеет значения, **насколько защищенным вы** сделали пароль пользователя изначально: со временем пользователь обычно сам выбирает себе пароль. Чтобы затребовать достаточно сложный пароль, вы можете настроить *учетные политики* (account policies) — подмножество политик, конфигурируемое как групповая политика.

Настройка учетных политик

Вы можете применять групповые политики на разных уровнях внутри сетевой структуры. (Об управлении локальными групповыми политиками и глобальными групповыми политиками см. главу 4.)

В контейнере групповой политики вы можете настроить учетные политики.

1. Раскройте узел учетных политик, переходя вниз по дереву консоли (рис. 8-1). Для этого раскройте узлы Computer

Configuration (Конфигурация компьютера), Windows Settings (Конфигурация Windows) и Security Settings (Параметры безопасности).

2. Теперь вы можете управлять учетными политиками через узлы Password Policy (Политика паролей), Account Lockout Policy (Политика блокировки учетных записей) и Kerberos Policy (Политика Kerberos).

Примечание Политики Kerberos не используются на локальных компьютерах. Они доступны только в групповых политиках, которые влияют на сайты, домены и ОП.

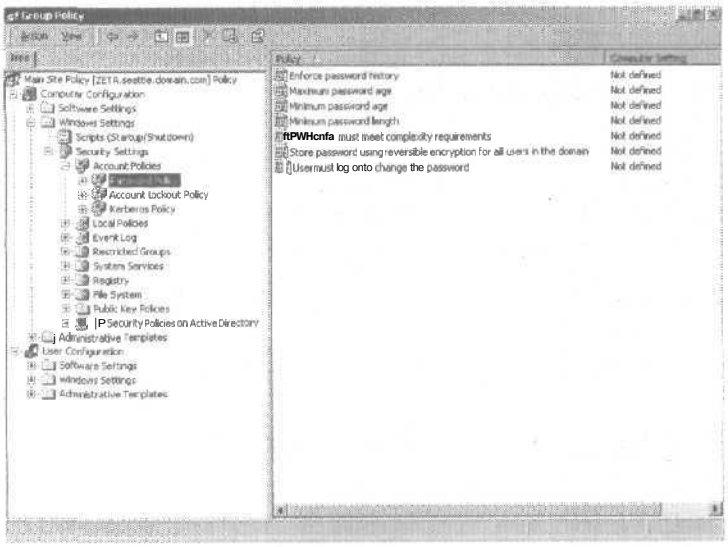


Рис. 8-1. Используйте элементы узла Account Policies (Политики учетных записей) для настройки политик паролей и общего назначения. В дереве консоли отображается имя компьютера или домен, который вы настраиваете.

3. Для настройки политики дважды щелкните соответствующую запись или, щелкнув ее правой кнопкой, выберите Security (Безопасность) — откроется окно свойств политики (рис. 8-2).
4. Действующая политика для компьютера отображается, но вы не можете изменить ее, Однако вы можете изменить

параметры локальной политики и тогда пропустите оставшиеся шаги — они применяются для глобальных групповых политик.

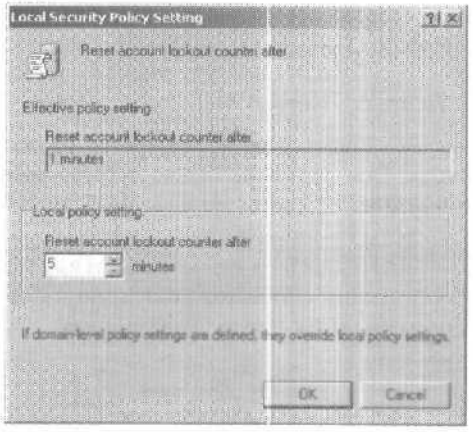


Рис. 8-2. Окно локальных политик позволяет просмотреть как действующую, так и локальную политики.

Примечание Политики сайтов, доменов и подразделений имеют приоритет над локальными политиками.

5. Окно свойств для сайтов, доменов или подразделений выглядит так (рис. 8-3):

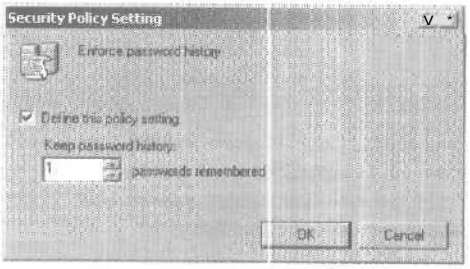


Рис. 8-3. Создавайте и конфигурируйте глобальные групповые политики из окна свойств.

6. Все политики могут быть либо определены, либо нет. Политика, не определенная в текущем контейнере, может быть унаследована от другого контейнера.

7. Чтобы включить политику, пометьте флажок Define This Policy Setting (Определить этот паарметр политики),

Примечание Политики имеют дополнительные поля для настройки ограничений, например переключатели Enabled (Включено) и Disabled (Выключено).

О работе с учетными политиками см. разделы «Настройка политики паролей», «Настройка политики блокировки учетной записи» и «Настройка политики Kerberos» этой главы.

Просмотр действующих политик

Работая с учетными политиками и назначениями прав пользователей, вы захотите просмотреть действующую политику на локальной системе, набор ограничений которой зависит от порядка применения политик по их иерархии (см. главу 4).

Рис. 8-4. В перечне локальных политик отображаются действующие политики, а также локальные.

Политику, действующую на локальной системе, можно просмотреть следующим образом.

1. Откройте узел локальной политики системы, как было описано в главе 4, или щелкните ярлык Local Policy Settings в меню Administrative Tools (если эти средства установлены и вы в данный момент подключены к компьютеру, который хотите изучить).
2. Раскройте узел политики, которую хотите просмотреть (рис. 8-4).

3. Для локальной политики вместо столбца Computer Setting отображаются столбцы Local Setting (Локальный параметр) и Effective Setting (Действующий параметр). В столбце Local Setting отображаются параметры локальной политики, а в столбце Effective Setting — параметры политики, примененные к на локальном компьютере.
4. Если вы увидите сообщения о конфликтах политик, см. главу 4.

Настройка учетных политик

Как вы уже знаете, существует три тина учетных политик: политики паролей, блокировки учетной записи и Kerberos.

Настройка политики паролей

Политики паролей управляют безопасностью паролей и позволяют задать следующие параметры:

- **Enforce Password History** (Требовать неповторяемости паролей);
- **Maximum Password Age** (Максимальный срок действия пароля);
- **Minimum Password Age** (Минимальный срок действия пароля);
- **Minimum Password Length** (Минимальная длина пароля);
- **Passwords** Must Meet **Complexity Requirements** (Пароли должны отвечать требованиям сложности);
- **Store Password Using Reversible Encryption For All Users In The Domain** (Хранить пароли всех пользователей в домене, используя обратимое шифрование).

Требовать неповторяемости паролей

Эта политика указывает, насколько часто старые пароли могут использоваться повторно. Она также может помешать пользователям менять пароли один на другой из одного общего набора. Windows 2000 может хранить до 24 паролей для каждого пользователя в предыстории паролей. По умолчанию Windows 2000 хранит один пароль в предыстории.

Чтобы отключить контроль предыстории, обнулите размер предыстории паролей, а чтобы включить — введите количество запоминаемых паролей в поле Passwords Remember. Windows 2000 будет отслеживать старые пароли, используя

предысторию, уникальную для каждого пользователя, и пользователям не будет разрешено применять заново любой из сохраненныхпаролей.

Примечание Вы можете помешать пользователям мошенничать с предысторией паролей, запретив им изменять пароли сразу: пользователь не сможет изменять пароль несколько раз подряд, чтобы вернуться к своему **старому** паролю.

Максимальный срок действия пароля

Параметр Maximum Password Age определяет, как долго пользователи могут применять пароли, прежде чем изменить их. Это делается с целью заставить пользователей периодически изменять свои пароли. Значение этого параметра определяется потребностями вашей сети. Чем важнее безопасность, тем короче должен быть период действия.

Вы можете задать период от 0 до 999 дней (по умолчанию — 42 дня). О означает, что срок действия пароля не ограничен, При высоких требованиях к безопасности рекомендуется требовать смену пароля каждые 30–90 дней. В остальных случаях — через 120-180 дней.

Примечание Windows 2000 уведомляет пользователей, когда срок **действия** пароля подходит к концу. Когда остается меньше 30 дней, пользователи при входе в сеть видят предупреждение о необходимости сменить пароль до истечения **срока.**

Минимальный срок действия пароля

Параметр Minimum Password Age определяет, как долго пользователи должны применять пароль, прежде чем смогут изменить его. Этот параметр позволяет помешать пользователям мошенничать с системой паролей, вводя новый пароль, а затем изменяя его на старый.

По умолчанию Windows 2000 позволяет пользователям изменять свой пароль сразу, но вы вправе задать определенный минимальный срок, Рекомендуемое значение — 3-7 дней.

Минимальная длина пароля

Параметр Minimum Password Length задает минимальное количество символов для пароля. Если вы до сих пор не

изменили параметр по умолчанию, срочно сделайте это, поскольку по умолчанию разрешены пустые пароли (т. с. вход в систему вообще без пароля).

Как правило, длина пароля составляет не менее 8 символов. Дело в том, что длинные пароли обычно взломать труднее, чем короткие. Если хотите большей безопасности, задайте минимальную длину пароля в 14 символов.

Пароли должны отвечать **требованиям** сложности

Помимо простых паролей и учетных политик, в Windows 2000 есть средства дополнительного управления паролями. Они доступны в фильтрах паролей, которые можно установить на контроллере домена. Если вы уже установили фильтр паролей, включите параметр Passwords Must Meet Complexity Requirements. После этого пароли должны будут соответствовать требованиям безопасности фильтра.

Например, стандартный фильтр Windows NT (PASSFILT.DLL) заставляет использовать защищенные пароли, т. е.:

- длина пароля — минимум 6 символов;
- пароль не содержит имени или части имени пользователя;
- в пароле применяются три из четырех доступных типов символов: буквы нижнего и верхнего регистров, цифры и знаки.

Хранить **пароли всех пользователей в домене, используя обратимое шифрование**

Пароли, хранимые в БД паролей, зашифрованы. Это шифрование обычно необратимо. Чтобы сделать его обратимым, включите параметр Store Password Using Reversible Encryption For All Users In The Domain. При этом пароли сохраняются с обратимым шифрованием и в случае необходимости могут быть восстановлены. Если же пользователь забыл свой пароль, администратор вправе его изменить.

Настройка политики блокировки учетных записей

К политикам блокировки учетных записей в домене или на локальной системе относятся:

- **Account Lockout Threshold** (Максимальное число неудачных попыток);
- **Account Lockout Duration** (Продолжительность блокировки учетной записи);

- **Reset Account Lockout Threshold After (Частота сброса** счетчика неудачных попыток).

Максимальное число неудачных попыток

Параметр Account Lockout Threshold определяет количество попыток входа в сеть. Установите его значение таким, чтобы оно сбалансировало потребность предотвращения взлома учетной записи и потребности пользователей, которым не удается сразу получить доступ к своим учетным записям.

Обычно пользователь не может получить доступ к своей учетной записи из-за того, что забыл пароль, и тогда он пытается войти в сеть еще несколько раз. У пользователей рабочих групп также могут быть проблемы с доступом на удаленную систему, где их текущий пароль не совпадает с тем, что ожидается удаленной системой. Если это случается, несколько неправильных попыток входа в сеть могут быть записаны удаленной системой прежде, чем пользователь получит приглашение ввести правильный пароль. Дело в том, что Windows 2000 может попытаться автоматически войти на удаленную систему. В среде домена этого обычно не происходит, благодаря функции однократного ввода пароля.

Возможные значения порога блокировки — от 0 (по умолчанию) до 999. О означает, что учетные записи не будут блокированы в случае неверных попыток входа в сеть. Любое другое значение задает порог блокировки: чем выше его значение, тем выше риск взлома вашей систему. Рекомендуемый диапазон значений для порога — от 7 до 15: это позволяет исключить ошибку пользователя и в то же время помешать взломщикам.

Продолжительность блокировки учетной записи

Параметр Account Lockout Duration задает период времени, в течение которого учетная запись будет заблокирована. Возможные значения — от 1 до 99 999 минут. Значение О блокирует учетную запись неопределенное время: это лучшая политика безопасности, так как при этом только администратор может разблокировать учетную запись. Это должно предотвратить попытки взломщиков получить доступ к системе повторно и заставит пользователей, чьи учетные записи заблокированы, искать помощи у администратора. Таким образом, вы можете определить, что пользователь

делает неправильно, и помочь ему избежать проблем в дальнейшем.

Примечание После блокировки учетной записи откройте окно свойств учетной записи из консоли Active Directory Users And Computers (Active Directory — пользователи и компьютеры) и на вкладке Account (Учетная запись) сбросьте флажок Account Is Locked (Учетная запись заблокирована). Это разблокирует учетную запись.

Частота сброса счетчика неудачных попыток

После каждой неудачной попытки входа в сеть Windows 2000 увеличивает значение счетчика неправильных попыток входа. Параметр Reset Account Lockout Threshold After (Сброс счетчика блокировки учетной записи через) определяет, как долго сохраняется значение этого счетчика. В исходное состояние это значение возвращается двумя путями: если пользователь вошел в сеть успешно или с момента последней неудачной попытки прошло время, указанное в параметре Reset Account Lockout Threshold After.

По умолчанию значение счетчика блокировки сохраняется 1 минуту, но вы можете задать интервал от 1 до 99 999 минут. Как и с порогом блокировки, нужно выбрать значение, которое сбалансирует потребности безопасности и удобства доступа. Рекомендуемое значение — 1-2 часа. Это заставит взломщиков ждать больше, чем они хотят, прежде чем попытаться получить доступ снова.

Примечание Неправильные попытки входа на рабочую станцию из хранителя экрана, защищенного паролем, не увеличивают значение счетчика. Аналогично, если вы заблокировали сервер или рабочую станцию, нажав Ctrl+Alt+Delete, неправильные попытки войти в сеть из диалогового окна разблокирования также не считаются.

Настройка политики Kerberos

Протокол Kerberos версии 5 — основной механизм аутентификации, используемый в домене Active Directory. Для проверки подлинности пользователей и сетевых служб протокол Kerberos применяет билеты, содержащие зашифрованные данные. Билеты служб необходимы служебным процес-

сам Windows 2000, а билеты пользователей — пользовательским процессам.

Вы можете контролировать срок действия билета и возможность его обновления посредством следующих политик:

- Enforce User Logon Restrictions;
- Maximum Lifetime For Service Ticket;
- Maximum Lifetime For User Ticket;
- Maximum Lifetime For User Ticket Renewal;
- Maximum Tolerance For Computer Clock Synchronization.

Внимание! Изменять эти параметры должны только администраторы, хорошо знакомые с **Kerberos.** Неправильная настройка этих параметров может вызвать серьезные проблемы в **сети. Как** правило, значения по умолчанию изменять не требуется.

Использовать ограничения для входа пользователя в сеть

Параметр Enforce User Logon Restrictions гарантирует применение любых ограничений, связанных с учетной записью пользователя. Так, если для пользователя ограничены часы входа в сеть, эта политика реализует это ограничение. По умолчанию этот параметр включен и должен отключаться только в исключительных случаях.

Максимальное время жизни

Параметры Maximum Lifetime For Service Ticket и Maximum Lifetime For User Ticket задают максимальное время, в течение которого действительны служебные или пользовательские билеты. По умолчанию максимальное время жизни служебных билетов — 41 760 минут, а пользовательских — 720 часов.

Вы можете изменить длительность действия билетов. Для служебных билетов диапазон составляет 0-99 999 минут, а для пользовательских — 0-99 999 часов. Нулевое значения параметра соответствует неограниченному сроку жизни.

Билет, время жизни которого истекло, может быть возобновлен, если это происходит в интервале из параметра Maximum Lifetime For User Ticket Renewal. По умолчанию максимальный период восстановления — 60 дней, допустимый интер-

вал — 0–99 999 дней. Значение 0 соответствует неограниченному периоду восстановления.

Максимальное отклонение

Параметр Maximum Tolerance For Computer Clock Synchronization — один из немногих, который вам, вероятно, понадобится изменить. По умолчанию компьютеры в домене должны быть синхронизированы друг с другом с точностью до 5 минут, иначе аутентификация невозможна.

Если у вас есть пользователи, которые входят в домен без синхронизации с сервером времени, задайте значение в интервале 0-99 999.

Настройка политик прав пользователя

В главе 7 мы обсуждали встроенные возможности и права пользователя. Встроенные возможности учетных записей изменять нельзя, но вы можете управлять правами пользователя для учетных записей. Вы можете делать пользователей членами соответствующей группы или групп. Вы также можете управлять правами пользователя для учетных записей.

Примечание Любой член группы, которой назначено определенное право, тоже имеет это право. Так, если группа Backup Operators имеет какое-либо право и TJSMITH является членом этой группы, он также имеет это право. Сделанные вами изменения в правах пользователя могут иметь далеко идущие последствия. Поэтому изменять политику прав пользователя должны только опытные администраторы.

Вы можете назначать права пользователя через узел Local Policies (Локальные политики) консоли групповых политик. Как и подразумевает имя, локальные политики принадлежат локальному компьютеру. И все же вы можете настраивать локальные политики, а затем импортировать их в Active Directory. Вы также можете настраивать эти локальные политики как часть существующей групповой политики для сайта, домена или подразделения, тогда они применяются к учетным записям компьютеров в сайте, домене или подразделении.

Политиками прав пользователя управляют так.

!. Раскройте нужный вам контейнер групповой политики и получите доступ к узлу Local Policies (Локальные поли-

тики). Раскройте пункты Computer Configuration (Конфигурация компьютера), Windows Settings (Конфигурация Windows) и Local Policies (Локальные политики).

2. Раскройте пункт User Rights Assignment (Назначение прав пользователя) (рис. 8-5).

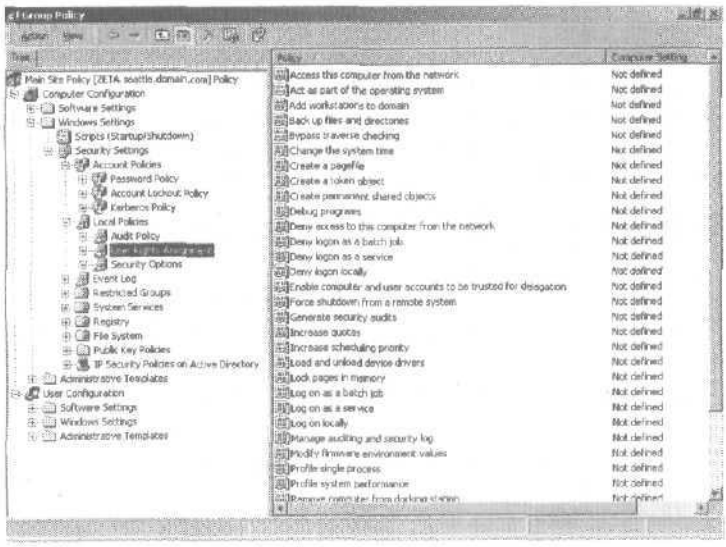


Рис. 8-5. Пункт User Rights Assignment служит для конфигурации прав пользователя для текущего контейнера групповой политики.

3. Для конфигурации назначения прав пользователя дважды щелкните права пользователя или, щелкнув их правой кнопкой, выберите в контекстном меню Security (Безопасность) — откроется диалоговое окно свойств.

1. Теперь вы можете настраивать права пользователя как описано в пп. 1-4 раздела «Локальная конфигурация нрав пользователя» или в пп. 1-7 следующего раздела.

Глобальная конфигурация прав пользователя

Вы можете настраивать индивидуальные права пользователя на уровне сайта, домена или подразделения.

1. Откройте диалоговое окно свойств для прав пользователя (рис. 8-6).

Примечание Все политики настроены для применения либо нет. Политика, не определенная в текущем контейнере, может быть наследована от другого контейнера.

Рис. 8-6. Определитз право пользователя, а затем примените его к пользователям или группам.

2. Пометьте флажок Define This Policy Settings для определения политики.

Для применения права к пользователю или группе щелкните кнопку Add (Добавить). Затем в диалоговом окне Group Name (Имя группы) щелкните кнопку Browse (Обзор) — откроется диалоговое окно Select Users Or Groups (рис. 8-7). Теперь можно применять право к пользователям или группам. Поля этого диалогового окна позволяют сделать следующее.

- **Look In** (Искать в) — получить доступ к именам учетных записей с других доменов. Щелкните окно списка Look In, где вы увидите текущий домен, доверенные домены и другие ресурсы, к которым вы можете получить доступ. Выберите пункт Entire Directory (Вся пайка) для просмотра всех имен учетных записей в каталоге.

Примечание В списке Look In перечислены только доверенные домены. Из-за транзитивных доверительных отношений в Windows 2000 это обычно означает, что просмат-

риваются все домены в *дереве доменов* (domain tree) или в лесу (forest). Переходящее доверие не устанавливается явно. Вернее, доверие устанавливается автоматически на основе структуры леса и прав, заданных в лесу.

- Name (Имя) отображает доступные учетные записи выбранного домена или ресурса.
- Add (Добавить) добавляет имена в список выбранного.
- Check Names (Проверить имена) позволяет подтвердить правильность имен пользователей и групп, введенных и список выбора. Это удобно, если вы вводите имена вручную и хотите удостовериться, что они доступны.

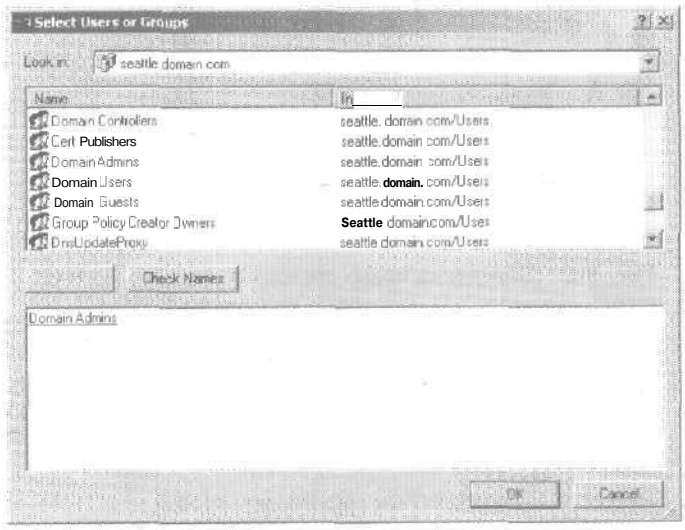


Рис. 8-7. Диалоговое окно Select Users Or Groups позволяет применить права пользователя к пользователям и группам.

3. Выбрав имена учетных записей для добавления в группу, щелкните OK. Теперь в окне Group Name должны отображаться выбранные учетные записи. Щелкните OK.
4. Диалоговое окно свойств обновится, отображая ваш выбор. Если вы допустили ошибку, выберите имя и удалите его, щелкнув кнопку Remove (Удалить).
5. Назначив права пользователям и группам, щелкните OK.

Локальная конфигурация прав пользователя

На локальных компьютерах права пользователя применяются так.

1. Откройте диалоговое окно свойств (рис. 8-8).

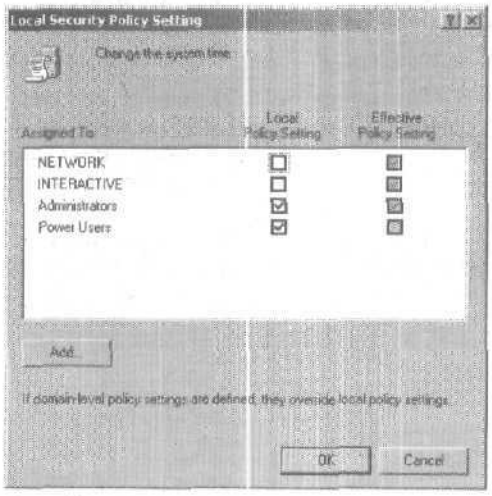


Рис. 8-8. Определив право пользователя, примените его к пользователям или группам.

2. Действующая политика для этого компьютера отображается, но вы не можете изменить ее. Однако вы можете изменить параметры локальной политики. Используйте поля диалогового окна, предназначенные для настройки локальной политики.

   Помните, что политики сайтов, доменов или подразделений имеют приоритет над локальными политиками.

3. В колонке Assigned To (Назначен) отображаются имена пользователей и групп, которым было дано право пользователя. Пометьте/сбросьте соответствующий флажок под колонкой Local Policy Setting для применения/отмены права пользователя.

Вы можете применить право пользователя другим пользователям и группам, щелкнув кнопку Add. В открывшемся окне Select Users Or Groups (рис. 8-7) можно добавить пользователей и группы.

Добавление учетной записи пользователя

Вам понадобиться создать учетную запись для каждого пользователя, который хочет обращаться к вашим сетевым ресурсам. Вы можете создать доменную учетную запись пользователя в консоли Active Directory Users And Computers (Active Directory — пользователи и компьютеры), а локальную учетную запись пользователя — из консоли Local Users And Groups (Локальные пользователи и группы).

Создание доменной учетной записи пользователя

Создать новые доменные учетные записи можно двумя способами.

- Создание полностью новой учетной записи пользователя. Щелкните правой кнопкой контейнер, в который вы хотите поместить учетную запись пользователя, выберите в контекстном меню New (Создать), а затем — User (Пользователь). Откроется окно мастера New Object — User (Новый объект — пользователь) (рис. 8-9). К созданной учетной записи применяются системные параметры по умолчанию.
- **Создание новой учетной записи на основе существующей.** Вызовите контекстное меню правым щелчком учетной записи пользователя, которую вы хотите скопировать в консоль Active Directory Users And Groups, и выберите Copy (Копировать). Откроется мастер Copy Object — User, похожий на диалоговое окно New User (Новый пользователь). Созданная копия учетной записи получает большинство значений параметров от существующей. О копировании учетных записей см. главу 9.

С помощью мастеров New Object — User или Copy Object — User учетная запись создается так.

1. Первое окно мастера позволяет ввести отображаемое имя пользователя и его имя для входа (рис. 8-9).
2. Введите имя и фамилию пользователя в соответствующих полях. Эти данные нужны для создания полного имени, которое и будет отображаемым именем пользователя.
3. Отредактируйте полное имя. Например, можно набрать его в формате Фамилия Имя Отчество, либо в формате Имя Отчество Фамилия. Полное имя должно быть уникальным в домене длиной не более 64 символа.

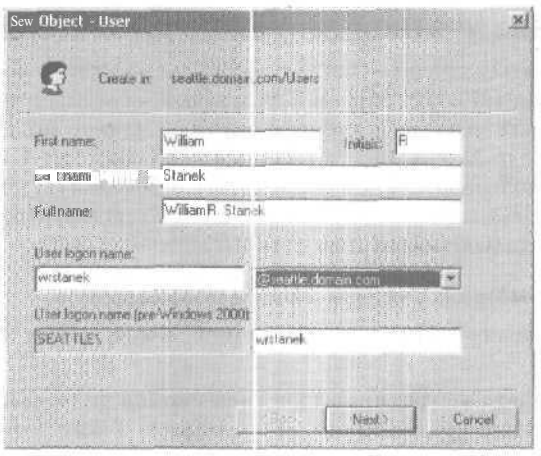


Рис. 8-9. Настройка отображаемого имени и имени для входа.

4. Наберите имя для входа в соответствующем поле. Далее используйте раскрывающийся список для выбора домена, с которым будет связана учетная запись. Это задает полное имя для входа.
5. Первые 20 символов имени для входа служат в качестве имени для входа в Windows NT версии 4.0 или более ранней. Это имя также должно быть уникальным в домене; при необходимости его можно изменить.
6. Щелкните Next (Далее). Укажите пароль для пользователя в открывшемся окне (рис. 8-10), параметры которого таковы:
   - Password (Пароль) — пароль для учетной записи; должен соответствовать вашей политике паролей;
   - Confirm **Password** (Подтверждение) — поле, используемое для подтверждения правильности введенного пароля: введите сюда пароль заново для его подтверждения;
   - **User** Must **Change Password** At Next Logon (Потребовать смену пароля при следующем входе в систему) — если отмечено, пользователь должен изменить пароль при следующем входе в систему;
   - **User** Cannot Change **Password** (Запретить смену пароля пользователем) — если отмечено, пользователь не может изменить пароль;

- **Password** Never **Expires** (Срок действия пароля не ограничен) — если отмечено, время действия пароля для этой учетной записи не ограничено; этот параметр перекрывает доменную политику учетных записей, (неограниченный по сроку действия пароль устанавливать не рекомендуется, так как это устраняет саму цель использования паролей);
- **Account Is Disabled** (Отключить учетную запись) - если отмечено, учетная запись заблокирована и не может быть использована; параметр удобен для временного запрета использования кем-либо этой учетной записи.

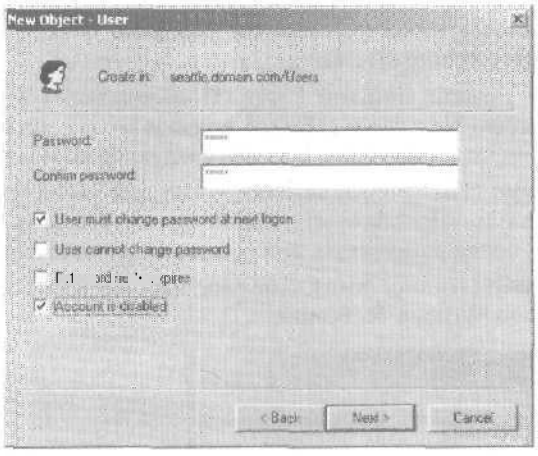


Рис. 8-Ю. Настройка пароля пользователя.

7. Щелкните Next, а затем Finish (Готово). Если возникли проблемы при создании учетной записи, вы увидите предупреждение. Вернитесь тогда к редактированию, щелкнув кнопку Back (Назад), и заново наберите информацию о пользователе и пароле.

Для созданной учетной записи можно установить расширенные свойства (см. главу 9).

Создание локальных учетных записей пользователя

Для создания локальных учетных записей служит консоль Local Users And Groups (Локальные пользователи и группы).

1. Выберите Start\Programs\Administrative Tools\Computer Management (Пуск\Программы\ Администрирование\Управление компьютером), либо выберите Computer Management (Управление компьютером) из папки Administrative Tools (Администрирование).
2. Щелкните правой кнопкой Computer Management (Управление компьютером) в дереве консоли и выберите в меню Connect To Another Computer (Подключиться к другому компьютеру). Теперь вы можете выбрать систему, локальными учетными записями которой будете управлять. На контроллерах домена нет локальных пользователей и групп.
3. Разверните ветвь System Tools (Служебные программы), щелкнув значок плюс (+), а затем выберите Local Users And Groups (Локальные пользователи и группы).
4. Щелкните правой кнопкой Users (Пользователи) и выберите в меню New User (Новый пользователь). Откроется одноименное окно (рис. 8-11) со следующими полями:
   - **Username** (Имя пользователя) — имя для входа учетной записи пользователя; должно соответствовать политике назначения имен локальным пользователям;
   - **Full** Name (Полное имя) — полное имя пользователя, например William R. Stanek;

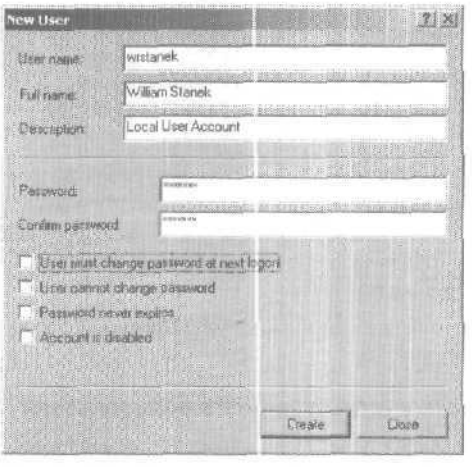


Рис. 8-11. Настройка локальной учетной записи пользователя отличается от доменной.

- **Description** (Описание) — дополнительная информация о пользователе; обычно сюда записываются сведения о должности, названии отдела и т. д.;
- **Password** (Пароль) — пароль для учетной записи; должен соответствовать условиям политики паролей;
- **Confirm Password** (Подтверждение пароля) — поле для подтверждения правильности введенного выше пароля; заново введите пароль в это поле;
- **User Must Change Password At Next Logon** (Потребовать смену пароля при следующем входе в систему) — если отмечено, пользователь должен изменить пароль при следующем входе в систему;
- User Cannot **Change Password** (Запретить смену пароля пользователем) — если отмечено, пользователь не может самостоятельно изменить пароль;
- **Password Never Expires** (Срок действия пароля не ограничен) — если отмечено, время действия пароля для этой учетной записи не ограничено; этот параметр перекрывает локальную политику учетных записей;
- **Account Is Disabled** (Отключить учетную запись) — если отмечено, учетная запись заблокирована и не может быть задействована; это поле удобно для временного запрета использования кем-либо учетной записи.

5. Закончив настройку новой учетной записи, щелкните Create (Создать).

Добавление учетной записи группы

Учетные записи групп позволяют управлять привилегиями нескольких пользователей. Вы можете создавать глобальные учетные записи групп в консоли Active Directory Users And Computers, а локальные — в консоли Local Users And Groups.

Помните, что вы создаете учетные записи групп для похожих типов пользователей. Можно выделить следующие типы групп.

- Группы **по отделам организации.** Сотрудники одного отдела обычно нуждаются в доступе к одним и тем же ресурсам. Поэтому вы можете создавать группы по отделам, таким как отдел развития бизнеса, отдел продаж, производственный отдел.

- **Группы по приложениям.** Зачастую пользователям нужен доступ к одному приложению и ресурсам для этого приложения. Если вы создаете группы, ориентированные на определенные приложения, убедитесь, что пользователи получают доступ к необходимым ресурсам и файлам приложения.
- Группы по должностям в организации. Группы могут быть организованы по должностям пользователей в организации. Так, должностным лицам, возможно, нужны ресурсы, к которым не обращаются другие пользователи. Создавая группы, основанные на должностях, вы даете пользователям доступ к ресурсам, в которых они нуждаются.

Создание глобальной группы

Глобальная группа создается так.

1. Запустите консоль Active Directory Users And Computers. Щелкните правой кнопкой контейнер, в который хотите поместить учетную запись пользователя. Выберите New, а затем Group (Группа). Откроется диалоговое окно New Object — Group (Новый объект — группа) (рис. 8-12).

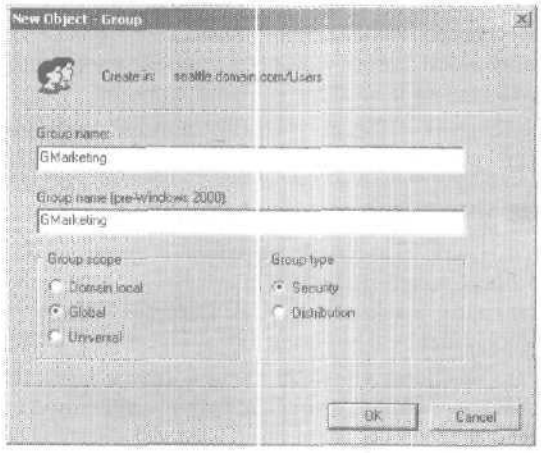


Рис. 8-12. Диалоговое окно New Object — Group позволяет добавлять новые глобальные группы в домен.

2. Введите имя группы. Имена глобальных учетных записей групп следуют тем же правилам, что и отображаемые

имена для учетных записей пользователей. Они нечувствительны к регистру и могут содержать до 64 символов.

3. Первые 20 символов имени группы будут соответствовать имени группы в Windows NT версии 4.0 и более ранних версий. Это имя группы должно быть уникальным в домене. Если нужно, измените его.
4. Выберите область видимости группы — Domain Local (Локальная в домене), Global (Глобальная) или Universal (Универсальная).
5. Выберите тип группы: Security (Группа безопасности) или Distribution (Группа распространения).
6. Щелкните OK. Как только учетная запись будет создана, вы можете добавлять членов группы и устанавливать дополнительные свойства.

Создание локальных групп и выбор членов группы

Локальные группы создаются в консоли Local Users And Groups.

1. **Выберите** Start\Programs\Administrative Tools\Computer Management (Пуск\Программы\ Администрирование\Управление компьютером). Либо выберите Computer Management (Управление компьютером) из папки Administrative Tools (Администрирование).
2. Щелкнув правой кнопкой Computer Management (Управление компьютером) в дереве консоли, выберите Connect To Another Computer. Теперь можно выбрать систему, локальными учетными записями которой вы будете управлять. На контроллере домена нет локальных пользователей и групп.
3. Разверните ветвь System Tools (Служебные программы), щелкнув значок плюс (+) и выберите пункт Local Users And Groups (Локальные пользователи и группы).
4. Щелкнув правой кнопкой Groups (Группы), выберите New Group (рис. 8-13).

   Введите имя и описание группы и щелкните кнопку Add, чтобы добавить имена в группу — откроется окно Select Users Or Groups (рис. 8-7).
5. Выбрав имена учетных записей для добавления в группу, щелкните OK.

Рис. 8-13. Диалоговое окно New Group позволяет добавлять новые локальные группы на компьютер.

6. Диалоговое окно New Group обновится, отображая ваш выбор. Если вы допустили ошибку, выберите имя и удалите его, щелкнув кнопку Remove (Удалить).
7. Завершив добавлять или удалять членов группы, щелкните Create (Создать).

Управление членством в глобальных группах

Для настройки членства служит консоль Active Directory Users And Computers. Работая с группами, помните, что;

- все новые пользователи домена являются Domain Users (Пользователи домена) — это их основная группа;
- все новые рабочие станции и службы домена являются Domain Computers (Компьютеры домена) — это их основная группа;
- все новые контроллеры домена являются Domain Controllers (Контроллеры домена) — это их основная группа.

Консоль Active Directory Users And Computers позволяет:

- управлять индивидуальным членством;
- управлять множественным членством;

- настраивать основную группу для отдельных пользователей и компьютеров.

Управление индивидуальным членством

Вы можете добавить в группу любой тип учетной записи.

1. Дважды щелкните имя пользователя, компьютера или группы в консоли Active Directory Users And Computers.
2. В окне свойств выберите вкладку Member Of (Член групп).
3. Чтобы сделать учетную запись членом группы, щелкните Add (Добавить). Откроется окно Select Groups, сходное с окном Select Users Or Groups. Теперь вы можете выбрать группы, к которым будет принадлежать текущая учетная запись.
4. Чтобы удалить учетную запись из группы, выберите группу и щелкните Remove (Удалить).
5. Щелкните OK.

Управление множественным членством

Членством в группе можно управлять и через диалоговое окно свойств группы.

1. Дважды щелкните название группы в консоли Active Directory Users And Computers. Откроется окно свойств группы.
2. Выберите вкладку Members (Члены группы).
3. Для добавления учетных записей в группу щелкните Add (Добавить). Откроется окно Select Users Or Groups. Теперь можно выбрать пользователей, компьютеры и группы, которые должны быть членами текущей группы.
4. Для удаления членов группы выберите учетную запись и щелкните Remove (Удалить).
5. Щелкните OK.

Настройка основной группы для пользователей и компьютеров

Основная группа назначается файлам или папкам, созданным пользователями Windows 2000 через службы для Macintosh. Все учетные записи пользователей и компьютеров должны иметь основную группу независимо от того, получает учетная запись доступ к системе Windows 2000 через служ-

бы для Macintosh или нет. Эта группа должна быть глобальной или универсальной, такой как **глобальная** группа Domain Users (Пользователи домена) или глобальная группа Domain Computers (Компьютеры домена). Основная группа настраивается так.

1. Дважды щелкните имя пользователя, компьютера или группы в окне консоли Active Directory Users And Computers. Откроется окно евойств.
2. Выберите вкладку Member Of (Член групп).
3. В списке членов выберите группу с глобальной или универсальной областью видимости.
4. Щелкните кнопку Set **Primary Group.**

Все пользователи должны быть членами хотя бы одной основной группы. Вы не можете отменить членство в основной группе, пока не выберете другую основную группу для пользователя.

1. Выберите другую группу с глобальной или универсальной областью видимости в списке членства и щелкните кнопку Set Primary Group.
2. В этом же списке выберите предыдущую основную группу и щелкните кнопку Remove (Удалить). Теперь членство в группе отменено.

Глава 9

Управление учетными записями пользователей и групп

В идеале можно было бы создать пользовательские и групповые учетные записи и никогда больше к ним не обращаться. Но в реальности после формирования учетных записей надо потратить немало времени па управление ими.

Управление информацией о контактах пользователя

Пользовательские учетные записи могут содержать подробную связанную информацию о контактах, доступную каждому внутри доменного дерева или леса.

Настройка информации о контактах

Для каждой учетной записи пользователя можно определить информацию о контактах.

1. Двойной щелчок имени пользователя в консоли Active Directory Users And Computers (Active Directory — пользователи и компьютеры) откроет диалоговое окно свойств записи.
2. Заполните поля на вкладке General (Общие) (рис. 9-1):
   - First Name, Initials, Last Name — поля для ввода имени, инициалов и фамилии пользователя;
   - Display Name (Имя входа пользователя) определяет, как будет отображаться имя пользователя в Active Directory и при входе в систему;
   - **Description** (Описание) — описание пользователя;

- **Office** (Комната) — расположение пользователя в офисе;
- **Telephone** Number (Номер телефона) — номер основного служебного телефона; чтобы указать другие номера служебных телефонов этого пользователя, нажмите Other (Другие) и в диалоговом окне Phone Number (Others) [Номер телефона (другие)] введите дополнительные номера телефонов;
- **E-Mail** (Электронная почта) — служебный почтовый адрес пользователя.
- **Web Page** (Web-страница) — URL (универсальный указатель ресурса) домашней страницы пользователя, которая может находиться как в Интернете, так и в интрасети компании; вы можете указать прочие Web-страницы: щелкнув Other (Другие), в диалоговом окне Web Page Address (Others) [Адрес Web-страницы (Другие)] введите дополнительные адреса Web-страниц.

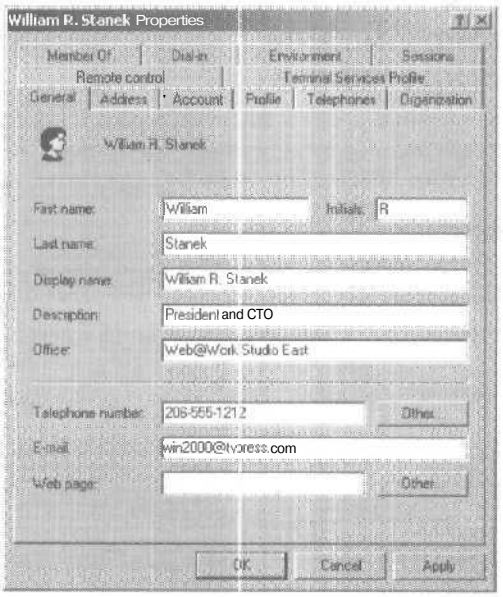


Рис. 9-1. На вкладке General можно сконфигурировать основную информацию о контактах пользователя, которая применяется в адресных книгах и при поиске.

Совет Чтобы задействовать функции отправки почты и открытия домашней страницы в консоли Active Directory Users And Computers, заполните поля E-Mail и Web Page. Подробности см. в разделе «Обновление учетных записей пользователей и групп».

3. **Выберите** вкладку Address **(Адрес).** Введите в **соответствующие поля рабочий и** домашний адрес **пользователя. Обычно вводят только рабочий адрес,** отмечая при этом **почтовый** адрес пользователя в **разных офисах.**

Примечание Прежде чем вводить домашний адрес пользователя, обсудите этот вопрос с отделом кадров и с юридическим отделом либо с самим пользователем.

4. Выберите вкладку Telephones (Телефоны). Введите основные номера контактных телефонов пользователя, например, домашнего, мобильного или IP-телефона, а также факса и пейджера.
5. Для каждого типа телефонного номера можно установить дополнительные номера. Щелкните кнопку Others (Другие) и, следуя инструкциям мастера, введите дополнительные номера телефонов.
6. Выберите вкладку Organization (Организация) и введите пользовательский заголовок, отдел и компанию, соответственно.
7. Чтобы указать руководителя пользователя, щелкните Change (Изменить), а затем в диалоговом окне Select User Or Contact выберите руководителя. После этого запись пользователя будет отображаться в графе прямых подчиненных руководителя.
8. Щелкните Apply (Применить) или OK, чтобы сохранить изменения.

Поиск пользователей и создание записей в адресной книге

Active Directory упрощает задачу поиска пользователей в каталоге и создания записей в адресной книге на основе результатов этого поиска.

1. Раскройте меню Start\Search (Пуск\Найти) и, щелкнув For People (Людей), откройте диалоговое окно (рис. 9-2).

2. В списке Look In (Искать в) выберите Active Directory и наберите имя или адрес электронной почты нужного пользователя.
3. Чтобы начать поиск, щелкните Find Now (Найти). Если поиск не завершится успехом, введите новые параметры и запустите поиск.
4. Выбрав из списка имя и щелкнув Properties (Свойства), можно посмотреть свойства записи.
5. Чтобы добавить информацию о контактах в адресную книгу, выберите имя и щелкните Add To Address Book (Добавить в адресную книгу).

Рис. 9-2. Поиск пользователей в Active Directory и создание записей к адресной книге.

Параметры среды пользователя

Пользовательские записи могут содержать профили, сценарии входа в систему и связанные домашние папки. Чтобы задать эти параметры, дважды щелкните имя в консоли Active Directory Users And Computers (Active Directory — пользователи и компьютеры) и выберите вкладку Profile (Профиль) (рис. 9-3), где можно заполнить следующие поля.

- Profile **Path** (Путь к профилю) — путь к профилю пользователя. Профили обеспечивают параметры среды пользователя. При каждом входе в систему профиль пользователя служит для определения параметров рабочего стола и панели управления, а также доступа к параметрам меню и приложениям, и так далее. Об установке пути профиля см. ниже раздел «Управление профилями пользователя».
- Logon **Script** (Сценарий входа) — путь к сценарию входа в систему пользователя. Сценарии входа — пакетные файлы, которые запускаются всякий раз при входе пользователя в систему. Сценарии входа позволяют определить команды, выполняемые при каждом входе пользователя в систему. О сценариях входа в систему см. главу 4.
- **Local Path** (Локальный путь) — папка, где хранятся файлы пользователя. Здесь можно указать каталог файлов пользователя, к которому он сможет обращаться с любого компьютера в пределах сети.

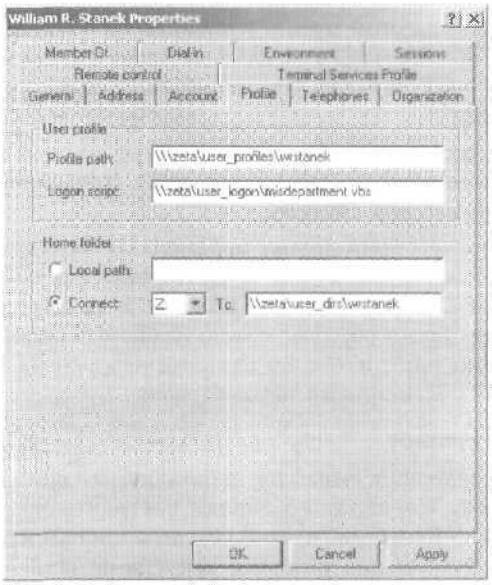


Рис. 9-3. Профиль пользователя задается на вкладке Profile. Профили позволяют конфигурировать сетевую среду пользователя.

Переменные системного окружения

Переменные системного окружения удобны для настройки среды пользователя, особенно при работе со сценариями входа в систему, и служат для определения динамически назначаемой информации о путях. Вот самые распространенные переменные окружения.

- *%SystemRoot%*— основной каталог ОС Microsoft Windows 2000 (например, C:\WIN2000). Используется на вкладке Profile (Профиль) диалогового окна свойств пользователя Properties (Свойства) и со сценариями входа в систему.
- *%UserName%*— имя пользователя в учетной записи (например, WRSTANEK). Используется на вкладке Profile (Профиль) окна свойств пользователя и со сценариями входа в систему.
- *%HomeDrive%* — буква диска домашней папки пользователя (например C:). Используется со сценариями входа в систему.
- *%HomePath%*— полный путь к домашней папке пользователя на соответствующем домашнем диске (например, \USERS\MKG\GEORGEJ). Применяется со сценариями входа в систему.
- *%Processor_Architecture%*— архитектура процессора компьютера пользователя (например, x86). Применяется со сценариями входа в систему.

Ниже показан пример применения переменных окружения при создании учетных записей (рис. 9-4). Переменная *%UserName%* позволяет ОС формировать полный путь для каждого пользователя. Таким образом можно назначить нескольким пользователям один и тот же путь, но каждый из них будет работать с собственными параметрами.

Сценарии входа в систему

Эти сценарии определяют команды, выполняемые при каждом входе в систему. Сценарии позволяют настроить системное время, сетевые принтеры, пути к сетевым дискам и т. д. Сценарии применяются для разового запуска команд; ими не следует изменять переменные окружения. Параметры среды, используемые сценариями, не сохраняются для последующих процессов. Не стоит также применять сценарии входа в систему для автоматического запуска приложений -

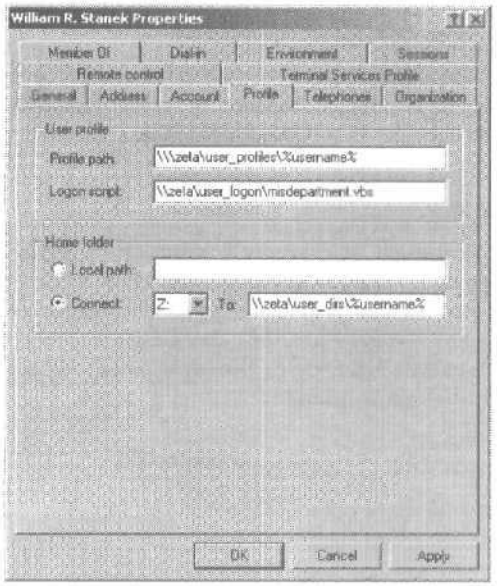


Рис. 9-4. На вкладке Profile переменные окружения позволяют вводить меньше данных, что особенно удобно при создании одной записи на основе другой.

лучше поместить соответствующие ярлыки в папку Startup (Автозагрузка).

Обычно сценарии входа в систему содержат команды Windows 2000. Но сценариями могут быть:

- файлы сервера сценариев Windows с расширениями .VBS, .JS и др.;
- пакетные файлы с расширением .BAT;
- командные файлы с расширением .CMD;
- программы с расширением .EXE.

Один сценарий может применяться как для одного, так и для нескольких пользователей; администратор определяет, с каким сценарием будет работать конкретный пользователь. Из названия очевидно, что пользователи обращаются к сценариям при входе в систему. Сценарий входа настраивается так.

1. В консоли Active Directory Users And Computers (Active Directory — пользователи и компьютеры) откройте окно

свойств пользователя и **выберите** вкладку **Profile** (Профиль).

2. В поле Logon Script (Сценарий входа) введите путь к сценарию. Убедитесь, что ввели полный путь к сценарию, например \\ZETA\USER_LOGON\ENG.VBS. •

Примечание Сценарии входа и выхода можно определить иначе — см. главу 4.

Практически любая команда, набранная в командной строке, может быть включена в сценарий входа. Наиболее типичные задачи, реализуемые в сценариях, — привязка принтеров и сетевых путей для пользователей, Эту задачу можно решить с помощью команды NET USE. Вот примеры команд привязки сетевого принтера и дисков:

```
net use lpt1: \\zeta\deskjet
net use g: \\gamma\corp\files
```

Если эти команды записаны в сценарий входа в систему, то сетевой принтер пользователя будет на порту LPT1, а сетевой диск получит букву G.

Назначение домашних папок

Windows 2000 позволяет назначить каждой учетной записи свою домашнюю папку для хранения и восстановления файлов пользователя. Большинство приложений открывают домашнюю папку для операций File Open (Открыть файл) и Save As (Сохранить как), что упрощает пользователям поиск своей информации. В командной строке домашняя папка является начальным текущим каталогом.

Домашняя папка может располагаться как на локальном жестком диске пользователя, так и на общедоступном сетевом. Каталог на локальном диске доступен только с одной рабочей станции, а к сетевому диску можно обращаться с любого компьютера сети, что расширяет среду пользователя.

Совет Несколько пользователей могут иметь одну домашнюю папку, но, как правило, лучше, чтобы у каждого пользователя была своя.

Создавать домашнюю папку специально не надо — ее автоматически создает консоль Active Directory Users And Computers. Но если это сделать не удастся, консоль предложит создать папку вручную.

Чтобы указать локальную домашнюю папку, сделайте так.

1. В консоли Active Directory Users And Computers откройте окно свойств пользователя и выберите вкладку Profile (Профиль).
2. Щелкните переключатель Local Path (Локальный путь) и введите путь к домашней папке, например **C:\Home** ***%UserName%***.

Сетевая домашняя папка определяется так.

1. В консоли Active **Directory** Users **And Computers** откройте окно **свойств** пользователя **и выберите** вкладку **Profile** (Профиль).
2. Щелкните переключатель Connect и выберите диск для домашней папки. Логично выбрать одну букву диска для всех пользователей. Убедитесь, что буква диска не будет конфликтовать с текущими локальными или сетевыми дисками. Чтобы избежать проблем, в качестве буквы диска выберите Z.
3. Введите полный UNC-путь к домашней папке, например: \\GAMMA\USER_DIRS\%UserName%. Чтобы обеспечить пользователю доступ к папке с любого компьютера сети, включите в путь имя сервера.

Примечание Если домашняя папка не указана, Windows 2000 будет использовать локальную домашнюю папку, заданную по умолчанию. На системах, обновленных до Windows 2000, эта папка — \Users\Default, на остальных - корневой каталог.

Параметры учетных записей

Windows 2000 предоставляет несколько способов управления записями пользователей и доступом пользователей с сеть. Можно назначить время входа в систему; компьютеры, с которых пользователи могут входить в систему; привилегии вызова по телефону и т. д.

Управление временем входа в систему

Windows 2000 позволяет настраивать и отслеживать время входа пользователей в систему. Время входа ограничивают для предохранения системы от взлома или иных злоумышленных действий по окончании рабочего дня.

В период действия времени входа в систему пользователи могут работать, как обычно: входить в сеть, обращаться к сетевым ресурсам. Если пользователи находятся в сети и их время входа истекло, произойдет то, что вы укажете в свойствах учетной записи:

- Forcibly disconnected — Windows 2000 принудительно отключит от всех сетевых ресурсов пользователей, время пребывания в системе которых истекло;
- **Not disconnected** — пользователи не отключаются от сети, но Windows 2000 не позволяет им производить новые сетевые соединения.

Конфигурирование времени входа в систему

Время входа в систему настраивается так.

1. В консоли Active Directory Users And Computers откройте диалоговое окно свойств пользователя и выберите вкладку Account (Учетная запись).
2. Щелкните кнопку Logon Hours (Время входа). В одноименном окне залайте разрешенное и запрещенное время входа в систему (рис 9-5). Параметры Logon Hours перечислены ниже (табл. 9-1).

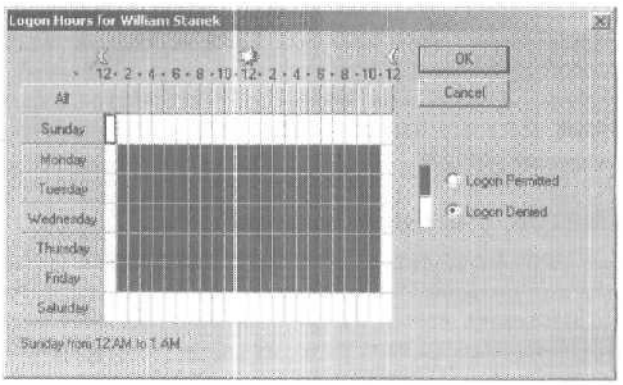


Рис. 9-5. В этом окне конфигурируется время входа в систему.

В этом диалоговом окне каждый час дня и ночи представлен в виде поля, который можно включить/выключить:

- разрешенные часы закрашены темным цветом, т. с. включены;

- запрещенные часы не закрашены, т. с. выключены.

Щелчок нужного часа изменяет его статус. Установите переключатель в положение Logon Permitted или Logon Denied.

Табл. 9-1. Параметры Logon Hours (Время входа в систему).

Параметр	Назначение
All (Все)	Позволяет выбрать все временные интервалы.
Кнопки дней недели	Позволяет выбрать все часы определенного дня.
Кнопки часов	Позволяет выбрать определенный час во всех днях недели.
Logon Permitted (Вход разрешен)	Устанавливает разрешенные часы пребывания в системе.
Logon Denied (Вход запрещен)	Устанавливает запрещенные часы пребывания в системе.

Совет Установив пользователям умеренно ограниченное время работы, вы сэкономите массу времени. Например, помимо стандартных часов (9–18), можно добавить несколько часов до и после рабочего дня. Тогда «жаворонки» смогут раньше входить в систему, а «совы» — продолжать работу после рабочего дня.

Жесткое время входа в систему

Пользователей, время пребывания в системе которых закончилось, можно отключить.

1. Откройте контейнер групповой политики, с которым хотите работать (см. главу 4).
2. *В* дереве консоли раскройте узел Computer Configuration\Windows Settings\Security Settings (Конфигурация компьютера\Параметры Windows\Параметры безопасности). Далее в Security Settings раскройте Local Policies (Локальные политики) и выберите Security Options (Параметры безопасности).
3. Двойной щелчок политики Automatically Log Off Users When Logon Time Expires (Автоматически отключать сеансы пользователей по истечении разрешенного времени) откроет окно ее свойств.
4. Щелкните Enabled (Включен), чтобы активизировать политику, а затем — OK.

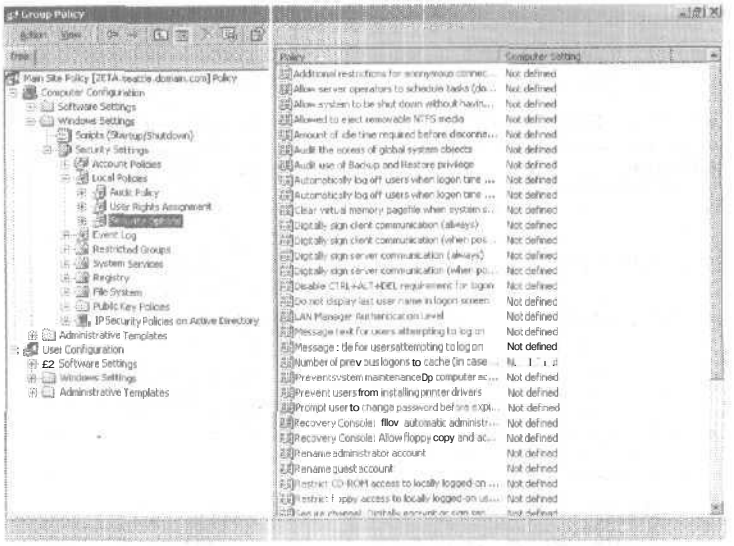


Рис. 9-6. Узел Security Options в оснастке Group Policy.

Настройка компьютеров, с которых пользователи входят в систему

Вы можете разрешать/запрещать пользователям работать на определенных компьютерах и входить с них в сеть. На рабочих станциях с Windows 2000 по умолчанию пользователям разрешается входить в домен с любого компьютера, по любой действующей учетной записи, включая гостевые записи.

Разрешая пользователям работать на любой рабочей станции, вы резко снижаете безопасность. Определив список разрешенных рабочих станций, вы закроете потенциальную брешь в защите домена. Теперь хакерам нужно найти не только пароль и имя пользователя, но и соответствующую рабочую станцию.

Примечание Внутри домена ограничение рабочих станций для входа в систему действует лишь при наличии Windows 2000 и Windows NT. На компьютеры с Windows 95 или Windows 98 эти ограничения не распространяются: для входа в систему требуется только пароль и имя пользователя.

Рабочие станции для входа в систему определяются так.

1. Раскройте окно свойств пользователя в консоли Active Directory Users And Computers и выберите вкладку Account (Запись).
2. Щелчок кнопки Log On To (Вход на) откроет диалоговое окно Logon Workstations (Рабочие станции для входа в систему).
3. Щелкните The Following Computers (Следующие компьютеры) (рис. 9-7).

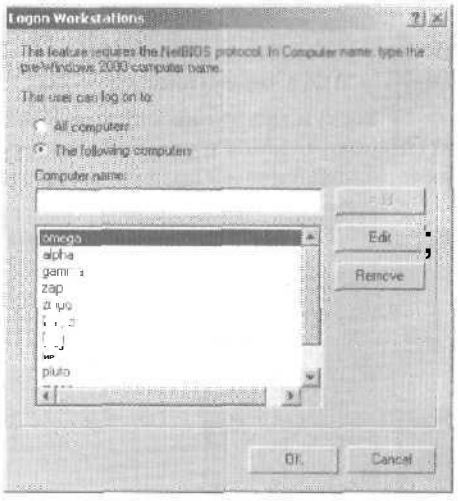


Рис. 9-7. Чтобы ограничить доступ к компьютерам, определите рабочие станции для входа в систему.

4. Введите имя рабочей станции и щелкните Add (Добавить). Чтобы указать несколько рабочих станций, повторите эту операцию.
5. Если вы ошиблись при заполнении, выберите ошибочную запись и щелкните Edit (Изменить) или Remove (Удалить).

Настройка привилегий вызова по телефону

На вкладке Dial-In (Входящие звонки) окна свойств пользователя можно настроить привилегии вызова но телефону. По умолчанию привилегии вызова по телефону управляются через Remote Access Policy (Политика удаленного доступа) (рис. 9-8). Можно предоставить/лишить привилегий, выб-

прав Allow Access (Разрешить доступ) или Deny Access (Запретить доступ). Прежде чем пользователь сможет дозвониться в сеть, сделайте так.

1. Установите службу Remote Access Services (Служба удаленного доступа) из программы Configure Your Server (Настройка сервера).
2. Чтобы включить соединения удаленного доступа, в узле Network Dial-Up And Connections (Сеть и удаленный доступ к сети) сконфигурируйте политику для места, домена или подразделения. Раскройте User Configuration\Administrative Templates\Network (Конфигурация пользователя\Административные шаблоны\Сеть) и выберите Network Dial-Up And Connections.
3. **Включите удаленный доступ, настроив** службу **Routing And Remote** Access (Маршрутизация и удаленный **доступ), В консоли Computer Management (Управление компьютером) раскройте** Services And **Applications (Службы и приложения) и выберите** Routing And **Remote Access.**

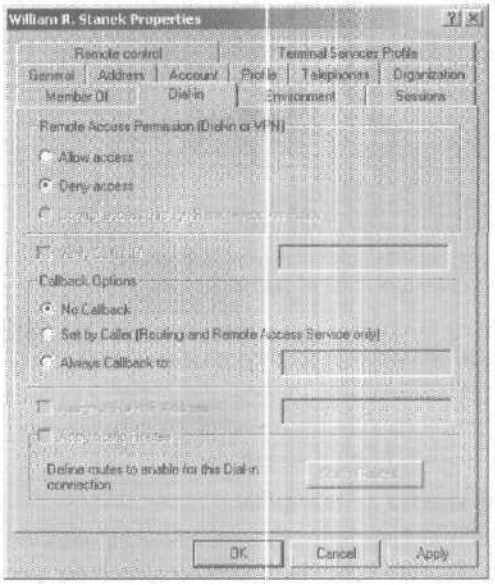


Рис. 9-8. Привилегии вызова по телефону регулируют удаленный доступ к сети.

После того как пользователь получил разрешение на удаленный доступ к сети, на вкладке Dial-In (Входящие звонки) окна свойств пользователя нужно настроить дополнительные параметры входящих звонков (рис. 9-8).

1. Если пользователь должен дозваниваться с определенного номера, выберите Verify Caller-ID (Проверять идентификатор), а затем введите номер телефона, с которого пользователь будет входить в систему. При этом ваша телефонная система должна поддерживать функции АОН (автоматического определения номера).
2. Определите параметры ответного вызова:

- **No Callback** (Ответный вызов не выполняется) — пользователь дозванивается, подключается и сам оплачивает телефонное соединение;
- **Set By Caller** (Устанавливается вызывающим) — сервер узнает номер телефона дозвонившегося пользователя, отключает его и звонит ему сам, при этом телефонное соединение оплачивает компания;

Примечание Назначать ответный вызов пользователям, которые дозваниваются через коммутатор не желательно. Коммутатор может помешать пользователю правильно подключится к сети.

- **Always Callback To** (Всегда по этому номеру) позволяет заранее указать номер повторного вызова с целью повышения безопасности; сервер перезванивает дозвонившемуся пользователю по этому номеру, компания оплачивает телефонное соединение.

Примечание Нельзя использовать предварительно назначенные номера повторного вызова на многоканальных линиях. Такие линии не будут работать надлежащим образом.

3. Можно указать статические IP-адреса и статические маршруты телефонных соединений в полях Assign A Static IP Address (Назначить статический IP-адрес) и Apply Static Routes (Назначить статические маршруты), соответственно. Об IP-адресах и маршрутизации см. главу 15.

Настройка параметров безопасности учетной записи

Вкладка Account (Учетная запись) окна свойств пользователя содержит массу параметров, которые применяются для

контроля применения учетных записей пользователей и для определения доступных параметров:

- User **Must Change Password** At **Next Logon** (Потребовать смену пароля при следующем входе в систему) заставляет пользователя сменить свой пароль при следующем входе;
- **User Cannot Change Password** (Запретить смену пароля пользователем) не позволяет пользователю изменять пароль;
- **Password Never Expires** (Срок действия пароля неограничен) гарантирует, что срок действия пароля никогда не истечет, т. е. отменяет нормальный срок действия пароля;

Внимание! Выбор этого параметра создает дополнительный риск для безопасности сети. Обычно его назначают для учетной записи администратора, но не для записей пользователей.

- **Store The Password Using Reversible Encryption** (Хранить пароль, используя обратимое шифрование) сохраняет пароль в виде зашифрованного текста;
- **Account Is Disabled** (Отключить учетную запись) отключает запись, не позволяя пользователю входить в систему и сеть;
- **Smart Card Is Required For Interactive Logon** (Для интерактивного входа в сеть нужна смарт-карта) требует смарт-карту для входа в систему; пользователь не может войти в систему, просто набрав имя и пароль.
- **Account Is Trusted For Delegation** (Учетная запись доверена для делегирования) определяет, требуются ли пользователю привилегии управления объектами в Active Directory, а также доверено ли ему производить какие-либо действия над объектами, для работы с которыми ему были делегированы соответствующие полномочия;

Примечание Не следует доверять делегирование большинству пользователей. Разрешайте это только тем, кому необходимо управлять Active Directory, или пользователям с особыми привилегиями.

- **Account Is Sensitive And Cannot Be Delegated** (Учетная запись важна и не может быть делегирована) определя-

ет, что пользователю нельзя доверять делегирование; этот параметр предотвращает управление компонентами Active Directory и обычно применяется ко всем учетным записям рядовых пользователей в отличие от вас и других полномочныхадминистраторов;

- **Use DES Encryption Types For This Account** (Использовать для этой учетной записи тины шифрования DES) определяет, будет ли запись пользователя применять стандарт шифрования DES;
- **Do Not Require Kerberos Preauthentication** (Без предварительной проверки подлинности Kerberos) — учетная запись пользователя перед получением доступа к сетевым ресурсам не нуждается в предварительной проверке подлинности Kerberos; предварительная проверка — часть процедуры безопасности Kerberos 5; вход в систему без такой проверки включается, чтобы идентифицировать пользователей предыдущей или нестандартной версии Kerberos.

Управление профилями пользователей

Профили пользователей содержат параметры сетевого окружения, такие как конфигурация рабочего стола, параметры меню. Проблемы, связанные с профилем, могут помешать пользователю войти в систему. Например, если размер экрана, заданный в профиле, не поддерживается системой, на которой он применяется, пользователь не сможет корректно войти в систему и не увидит ничего, кроме пустого экрана. Можно перезагрузить компьютер, перейти в режим VGA, после чего сбросить параметры дисплея вручную. Решить проблемы с профилем не всегда просто, иногда требуется изменить сам профиль.

Windows 2000 предоставляет несколько способов управления профилями:

- назначить путь к профилю в консоли Active Directory Users And Computers;
- копировать, удалять и изменять тип существующего локального профиля из панели управления с помощью программы System (Система);
- задать системные правила, которые не позволят пользователям всецело управлять своим окружением.

Локальный, перемещаемый и обязательный профили

В Windows 2000 каждый пользователь обладает профилем. Профили управляют параметрами запуска сеанса пользователя, типами доступных программ и приложений, параметрами рабочего стола и т. д. Каждый компьютер, на который входит пользователь, оснащен своей копией профиля пользователя. Профиль хранится на жестком диске компьютера; поэтому пользователь, работающий на нескольких рабочих станциях, должен обладать профилем на каждом из них. Другой компьютер сети не может обращаться к профилю, сохраненному локально, или *локальному профилю;* очевидно, что это имеет свои недостатки. Например, если пользователь работает на трех станциях, то на каждой системе у него могут быть разные профили. В результате пользователь может запутаться в том, какие сетевые ресурсы доступны ему на каждой из систем.

Чтобы уменьшить путаницу, можно создать профиль, доступный другим компьютерам, — *перемещаемый профиль. К* такому профилю пользователь может обращаться с любого компьютера домена. Перемещаемые профили основаны на сервере Windows 2000 и хранятся только там. При входе пользователя с перемещаемым профилем в систему загружается профиль, т. е. создается его локальная копия на компьютере пользователя. Когда пользователь выходит из системы, измененный профиль обновляется как на сервере, так и локально.

Администратор может управлять профилями пользователей или позволять им самим распоряжаться своими профилями. Управлять профилями самостоятельно можно лишь по одной причине: чтобы убедиться, что у всех пользователей одинаковые параметры сети. Это может снизить количество проблем, связанных с сетевой средой.

Профили, управляемые администраторами, называются *обязательными.* Пользователи с обязательными профилями могут производить лишь временные изменения своего окружения, которые не будут сохранены: при следующем входе в систему пользователь вернется к первоначальному профилю. Смысл в том, что пользователи не могут произвести необратимых изменений сетевой среды, т. е. изменений, ведущих к проблемам. Главный недостаток обязательных профилей в том, что пользователь может войти в систему, только если профиль доступен. Если сервер, на котором хранится про-

филь, а также кэшированный профиль недоступны, пользователь не сможет войти. Если недоступен только сервер, он получит предупреждение, но сможет войти на локальную систему Windows 2000 при помощи кэшированного системного профиля.

Создание локальных профилей

В Windows 2000 профили пользователей находятся либо в каталоге, заданном по умолчанию, либо в каталоге, указанном в поле Profile Path (Путь к профилю) в окне свойств пользователя. Стандартное расположение каталога профилей зависит от конфигурации рабочей станции.

- Обновление операционной системы до Windows 2000 - профиль пользователя расположен по адресу *%SystemRoot%*\Profiles*%UserName%*\NTUSER.DAT, где *%SystemRoot%* — корневой каталог ОС (например, C:\WINNT), а *%UserName%* — имя пользователя (wrstanek).
- Новая установка Windows 2000 — профиль пользователя расположен по адресу *%SystemDrive%*\Documentsand Settings*% UserName%.%UserDomain%*\NTUSER.DAT (например, F:\Documents and Settings\WRSTANEK.WEBATWORK\NTUSER.DAT). Если пользователь входит на контроллер домена, то профиль может быть расположен на *%SystemDrive%*\Documentsand Settings*% UserName%.<сервер входа>* (например, F:\Documents and Settings\WRSTANEK.ZETA\NTUSER.DAT).

Если не изменить каталог по умолчанию, пользователь будет работать с локальным профилем.

Создание перемещаемых профилей

Перемещаемые профили хранятся на серверах Windows 2000. Чтобы у пользователя был перемещаемый профиль, его каталог должен располагаться на сервере.

1. Создайте общий каталог на сервере Windows 2000 и убедитесь, что группа Everyone (Все) имеет к нему доступ.
2. В консоли Active Directory Users And Computers в окне свойств пользователя выберите вкладку Profile (Профиль). Введите путь к общему каталогу в поле Profile Path (Путь к профилю) в виде *\\имя_сервера\имя_папки_профиля\имя_пользователя* (например, \\ZETA\USER_PROFILES\

GEORGEJ), где ZETA - имя сервера, USER_PROFILES — общий каталог, а GEORGEJ — имя пользователя.

3. Перемещаемый профиль сохранится в файле NTUSER.DAT указанного каталога (например, \\ZETA\USER_PROFILES\GEORGEJ\NTUSER.DAT.)

Примечание Обычно создавать каталог профиля не требуется, так как он создается автоматически при входе пользователя в систему.

4. Необязательное действие: можно создать профиль пользователя или скопировать существующий профиль в папку профилей пользователя. Если фактический профиль пользователя не создан, то в следующий раз пользователь войдет в систему по стандартному локальному профилю. Любые изменения этого профиля будут сохранены, когда пользователь выйдет из системы. Таким образом, при очередном входе пользователь будет иметь личный профиль.

Создание обязательных профилей

Обязательные профили хранятся на серверах Windows 2000. **Чтобы назначить** пользователю обязательный **профиль,** сделайте так.

1. **Выполните пп. 1-3** раздела «Создание **перемещаемых** профилей».
2. Создайте обязательный профиль, переименовав файл NTUSER.DAT в *%USERNAME%*\NTUSER.MANТеперь при следующем входе в систему пользователь будет обладать обязательным профилем.

Примечание Файл NTUSER.DAT содержит пользовательские параметры системного реестра. Замена расширения файла на NTUSER.MAN заставляет Windows 2000 создать обязательный профиль.

Управление локальными профилями с помощью программы System

Для управления системными профилями нужно войти на компьютер пользователя и вызвать служебную программу System (Система) из Control Panel (Панель управления). Чтобы просмотреть текущий профиль, запустите System и перейдите на вкладку User Profiles (Профили пользователей).

Вкладка User Profiles отражает информацию обо всех профилях на локальной системе (рис. 9-9). Поля имеют следующие значения.

- **Name** (Имя) — имя локального профиля, которое обычно содержит имя первоначального домена или компьютера и имя записи пользователя. Например, имя WEBATWORK\WRSTANEK означает, что первоначальный профиль получен от домена WEBATWORK, а запись пользователя - WRSTANEK.

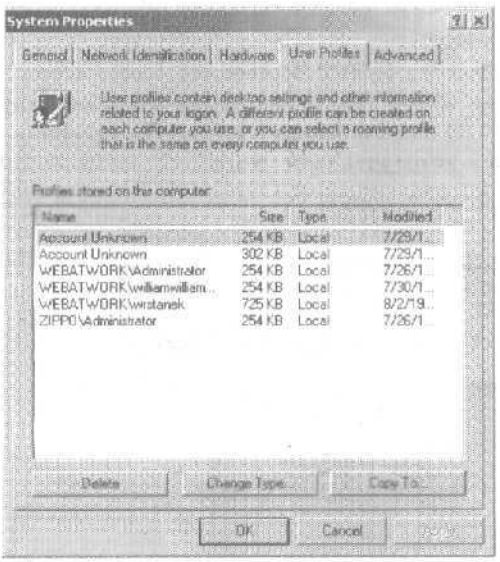


Рис. 9-9. Вкладка User Profiles позволяет управлять локальными профилями.

Если удалить учетную запись, не удаляя соответствующий профиль, можно увидеть строку Account Deleted (Запись удалена) или Account Unknown (Неизвестная запись). Не беспокойтесь, профиль все еще доступен для копирования.

- Size (Размер) —размер профиля. Обычно чем больше файл профиля, тем больше параметров окружения настроил пользователь.
- **Type** (Тип) — тип профиля: локальный или перемещаемый.
- Modified (Изменен) — дата последнего изменения профиля.

Создание профиля вручную

Чтобы создать профиль вручную, надо войти в систему по учетной записи пользователя, настроить среду и выйти. Так как это занимает много времени, лучше создать базовую запись пользователя, настроить ее среду, а затем применять ее как основу для других записей.

Копирование профиля в новую учетную запись пользователя

Вы можете скопировать существующий профиль в новую учетную запись. Сделать это позволяет программа System из панели управления.

1. Запустите System и перейдите на вкладку User Profile.
2. В списке Profiles Stored On This Computer (Профили, хранящиеся на этом компьютере) выберите профиль, который нужно скопировать (рис. 9-9).
3. Скопируйте профиль в новую учетную запись щелкнув кнопку Copy To (Копировать в). Затем введите путь нового каталога профилей пользователя в поле Copy Profile To (Копировать профиль на) (рис. 9-10). Например, если вы создали профиль для пользователя GEORGEJ, напечатайте **\\ZETA\USER_PROFILES\GEORGEJ**.

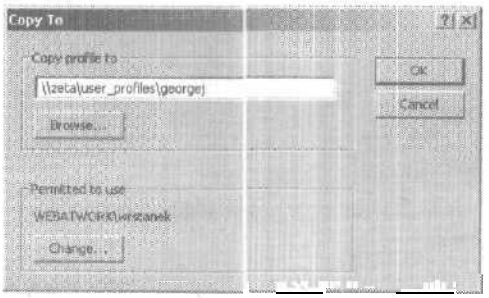


Рис. 9-10. Диалоговое окно Copy To позволяет ввести адрес каталога профиля и дать пользователю разрешение на доступ.

4. Теперь нужно разрешить пользователю доступ к профилю. Щелкните кнопку Change (Изменить) в области Permitted To Use (Разрешить использование) и в диалоговом окне Select User Or Object (Выбор: Пользователь или группа) разрешите доступ для новой учетной записи пользователя.

5. Щелкните OK, и Windows 2000 скопирует профиль в новый каталог.

Совет Если имя пользователя или группы известно, наберите его прямо в поле Name (Имя).

Копирование и восстановление профиля

При работе с рабочими группами, где каждый компьютер управляется независимо, приходится часто копировать профиль пользователя с одного компьютера на другой. Копирование профилей позволяет пользователям работать с едиными параметрами среды на разных компьютерах. Естественно, что в домене Windows 2000 для реализации перемещаемого профиля можно создать отдельный профиль, доступный из любой точки домена. Проблема в том, что иногда может понадобиться скопировать существующий локальный профиль поверх перемещаемого профиля пользователя (когда перемещаемый профиль поврежден), либо в перемещаемый профиль другого домена.

Вы можете скопировать существующий профиль в новый каталог.

1. Войдите на компьютер пользователя, запустите программу System из панели управления и перейдите на вкладку User Profile.
2. В списке Profiles Stored On This Computer выберите профиль, который нужно скопировать.
3. Скопируйте профиль в новый каталог, щелкнув кнопку Copy To, а затем в поле Copy Profile To введите путь к новому профильному каталогу. Например, при создании профиля для пользователя JANEW введите \\GAMMA\USERPROFILES\JANEW.
4. Теперь нужно открыть пользователю доступ к профилю. Щелкните кнопку Change (Изменить) в области Permitted To Use (Разрешить использование) и в окне Select User Or Object (Выбор: Пользователь или группа) разрешите доступ для новой учетной записи пользователя.
5. Щелкните OK, и Windows 2000 скопирует профиль в новый каталог.

Удаление локального профиля и назначение нового

В Windows 2000 пользователи, не имеющие перемещаемых профилей работают с локальными. Вообще локальные профили применяются, если у них более поздняя дата изменения, чем у перемещаемых. Например, если локальный профиль поврежден, его можно удалить и назначить новый. Однако, удаляя локальный профиль (если он нигде в домене не сохранен), вы потеряете первоначальные пользовательские параметры среды.

Локальный профиль пользователя можно удалить так.

1. Войдите на компьютер пользователя.
2. Запустите программу System (Система) и перейдите на вкладку User Profiles (Профили пользователя).
3. Выберите удаляемый профиль и щелкните Delete (Удалить). При запросе подтвердите удаление, щелкнув Yes (Да).

Примечание Нельзя удалить используемый профиль. Если пользователь работает на локальной системе (компьютер, с которого **вы** удаляете профиль), то ему следует выйти из системы. Иногда Windows 2000 маркирует профили как занятые, хотя на самом деле это не так. Обычно это происходит в результате некорректного изменения среды пользователя. Чтобы это исправить, перезагрузите компьютер.

При следующем входе пользователя в систему Windows 2000 произведет одну из двух операций: либо предоставит ему локальный профиль системы, заданный по умолчанию, либо найдет ее перемещаемый профиль на другом компьютере. Чтобы не назначать ни одного из этих профилей, пользователю нужно назначить новый. Для этого:

* скопируйте существующий профиль в каталог с профилями пользователя (см. об этом следующий раздел);
* обновите параметры профиля пользователя в консоли Active Directory Users And Computers (о настройке пути к профилю см. раздел «Параметры среды пользователя»).

Изменение типа профиля

Программа System позволяет изменять тип перемещаемых профилей на компьютере пользователя. Чтобы сделать это,

выберите профиль и щелкните Change Type (Сменить тип), Параметры диалогового окна позволяют сделать следующее.

- Активизировать локальный профиль, если нужно, чтобы пользователь всегда работал на этом компьютере с локальным профилем. Теперь все изменения профиля происходят локально, а первоначальный перемещаемый профиль остается нетронутым,
- Активизировать перемещаемый профиль, чтобы при следующем входе в систему пользователь работал с первоначальным перемещаемым профилем. Затем Windows 2000 будет обрабатывать этот профиль, как любой другой перемещаемый профиль, т. е, любые изменения в локальном профиле будут копироваться в перемещаемый.

Примечание Если эти параметры недоступны, то первоначальный профиль пользователя определен локально.

Обновление учетных записей пользователей и групп

Консоль Active Directory Users And Computers позволяет обновить доменную учетную запись пользователя или группы. Для обновления локальной учетной записи пользователя или группы служит оснастка Local Users And Groups (Локальные пользователи и группы).

Переименование учетных записей пользователей и групп

Учетную запись можно переименовать.

1. Раскройте консоль Active Directory Users And Computers или Local Users And Groups и найдите нужную учетную запись.
2. Щелкните ее правой кнопкой, выберите Rename (Переименовать) и введите новое имя.

Идентификаторы SID

При переименовании учетной записи пользователя назначается новая метка. Имена пользователей облегчают управление учетными записями (см. главу 7). Windows 2000 использует дескриптор безопасности SID для идентификации, отслеживания и обработки учетных записей независимо от имен

пользователей. SID — однозначный идентификатор, генерируемый при создании учетной записи.

Так как SID внутренне связан с учетными записями, нет нужды изменять разрешения и привилегии переименованных записей. Windows 2000 просто связывает SID с новым именем, если это необходимо.

Единственная причина переименования учетной записи — изменение его фамилии. Например, если Jane Williams (JANEW) вышла замуж, она может захотеть изменить свое имя на Jane Marshall (JANEM). При переименовании пользователя JANEW в JANEM все связанные с ним привилегии и разрешения отразят изменение имени. Таким образом, если раньше JANEW имела доступ к файлу, то теперь доступ открыт для JANEM (JANEW будет исключена из списка доступа).

Изменение другой информации

При переименовании JANEW в JANEM свойства пользователя и имена файлов, связанные с записью, не изменятся. Это значит, что вам следует обновить информацию об учетной записи. Информация, которая *может* быть изменена:

- Display Name — в консоли Active Directory Users And Computers (Active Directory — Пользователи и компьютеры) изменяет имя записи пользователя;
- User Profile Path — в Active Directory Users And Computers изменяет путь к профилю, а затем переименовывает соответствующий каталог на диске;
- Logon Script Name — если у каждого пользователя индивидуальный сценарий входа в систему, изменяет имя сценария входа в систему к Active Directory Users And Computers, а затем на диске переименовывает сценарий входа;
- Home Directory изменяет путь к домашнему каталогу в Active Directory Users And Computers, затем переименовывает соответствующий каталог на диске.

Примечание Если пользователь находится в системе, то изменение каталогов и файловой информации учетной записи может повлечь определенные проблемы. Поэтому обновление информации лучше производить в нерабочее время или попросить пользователя выйти из системы на некоторое время, а затем вновь войти.

Копирование доменных учетных записей пользователей

Создавать новые доменные учетные записи «на пустом месте» довольно утомительно. В качестве отправной точки можно использовать уже существующую запись.

1. В Active Directory Users And Computers щелкните правой кнопкой запись, которую нужно скопировать, и выберите Copy (Копировать). Откроется окно Copy Object — User.
2. Создайте учетную запись аналогично любой доменной записи пользователя. Затем обновите соответствующие свойства записи.

Вопреки ожиданиям при копировании учетной записи консоль Active Directory Users And Computers не сохранит всю информацию существующей учетной записи. Вместо этого Active Directory Users And Computers пытается скопировать только нужную информацию и пропустить данные, которые так или иначе потребуют обновления. Сохраняемые свойства включают:

- город, штат, индекс и набор стран на вкладке Address (Адрес);
- отдел и компания на вкладке Organization (Организация);
- параметры записи в нолях параметров учетной записи на вкладке Account (Учетная запись);
- время входа в систему и рабочие станции для входа в систему;
- срок действия учетной записи;
- членство в группах;
- параметры профиля;
- привилегии вызова по телефону.

Примечание **Если** для определения параметров профиля исходной учетной записи вы использовали переменные окружения, то они будут применяться и в копии учетной записи. Например, если в исходной записи использовалась переменная *%UserName%*, то **в** ее **копии** также будет применятся эта переменная.

Удаление учетных записей пользователей и групп

Удалив учетную запись, нельзя создать новую с таким же именем для получения тех же полномочий, поскольку SID новой записи не будет совпадать с SID старой.

Windows 2000 не позволяет удалять встроенные учетные записи пользователей *л* групп, так как их удаление может серьезно повлиять на домен. Чтобы удалить учетные записи других типов, надо выбрать их и нажать клавишу DEL, либо щелкнуть их правой кнопкой и выбрать Delete (Удалить), щелкнуть OK. а затем Yes (Да).

В Active Directory Users And Computers **можно** выбрать:

- несколько имен пользователей, удерживая нажатой клавишу Ctrl и последовательно щелкая каждую требуемую запись;
- диапазон имен пользователей, удерживая клавишу Shift и щелкнув сначала первую, а затем последнюю запись диапазона.

Примечание При удалении **учетной** записи, Windows 2000 не удаляет профиль пользователя, личные файлы и домашнюю папку. Эти файлы можно **удалить** вручную.

Изменение и переустановка паролей

Администратору приходится часто изменять или обнулять пароли пользователей. Обычно это требуется, когда пользователи забывают свои пароли либо если время действия их паролей истекло.

Вы можете изменить/сбросить пароль.

1. Войдите в консоль Active Directory Users And Computers или Local Users And Groups в зависимости от типа учетной записи, которую нужно переименовать.
2. Щелкните правой кнопкой имя записи и в контекстном меню выберите Reset Password (Смена пароля) или Set Password (Задать пароль).
3. Введите новый пароль пользователя и подтвердите его. Пароль должен соответствовать набору правил паролей компьютера или домена.
4. Дважды щелкните имя и снимите, если надо, флажки Account Is Disabled (Учетная запись отключена) и Account Is Locked Out (Учетная запись заблокирована). В Active

Directory Users And Computers эти флажки находятся на вкладке Account.

Включение учетных записей пользователей

Учетные записи пользователей могут быть отключены по нескольким причинам: пользователь забыл пароль и пытался угадать его; пользователь мог нарушить правила учетной записи; другой администратор мог отключить учетную запись, пока пользователь был в отпуске; срок действия учетной записи мог закончиться.

Учетная запись отключена

Если учетная запись отключена, сделайте так.

1. Войдите в консоль Active Directory Users And Computers или Local Users And Groups в зависимости от типа учетной записи, которую нужно переименовать.
2. Щелкните правой кнопкой имя учетной записи пользователя и в контекстном меню выберите Enable Account (Включить учетную запись).

Учетная запись заблокирована

Если учетная запись заблокирована, сделайте так.

1. Войдите в консоль Active Directory Users And Computers или Local Users And Groups (Локальные пользователи и группы) в зависимости от типа учетной записи, которую нужно переименовать.
2. Дважды щелкните имя учетной записи пользователя и снимите флажок Account Is Locked Out (Учетная запись заблокирована). В Active Directory Users And Computers этот флажок расположен на вкладке Account (Учетная запись).

Примечание Если пользователи часто блокируются, скорректируйте правила учетной записи домена. Можно увеличить значение приемлемых попыток входа в систему и уменьшить продолжительность хранения связанного счетчика. О настройке политики учетной записи см. главу 8.

Истек срок действия учетной записи

В отличие от учетных записей пользователей доменные учетные записи имеют дату истечения срока действия.

Если срок действия учетной записи истек, сделайте так.

1. Откройте консоль Active Directory Users And Computers.
2. Дважды щелкните имя учетной записи пользователя и перейдите на вкладку Account (Учетная запись).
3. На панели Account Expires (Срок действия учетной записи) выберите End Of (Истекает) и раскройте список. Появится календарь, в котором можно назначить новый срок действия.

Решение проблем входа в систему

Кроме типичных причин отключения учетной записи, некоторые системные параметры могут также помешать доступу.

- **Пользователь получил сообщение, что не может интерактивно войти в систему.** Для данного пользователя не определено право входа в систему, и он не является членом группы, обладающей таким правом.

  Пользователь может попытаться войти на сервер или доменный контроллер. Если так, учтите, что право локального входа применимо для всех доменных контроллеров внутри домена. Иначе это право применимо к отдельной рабочей станции.

  Если пользователь имеет доступ к локальной системе, сконфигурируйте право пользователя Logon Locally (Локальный вход), как описано в главе 8.

- **Пользователь получил сообщение, что система запретила ему вход.** Если пароль и учетное имя уже проверены, может потребоваться проверка типа учетной записи. Пользователь может пробовать получить доступ к домену через локальную учетную запись. Если проблема не в этом, то может быть недоступен сервер глобального каталога, в результате чего лишь пользователи с привилегиями администраторов смогут входить в систему.

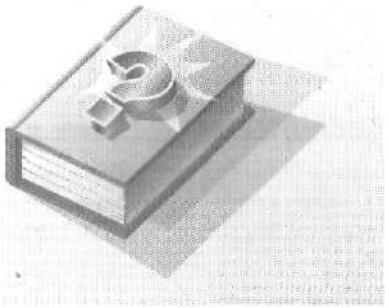
- **Пользователь обладает обязательным профилем, а компьютер, на котором он** хранится, **недоступен.** Если пользователь имеет обязательный профиль, то компьютер, на котором он хранится, должен быть доступен во время входа в систему. Если компьютер выключен или недоступен по другим причинам, то пользователи с обязательными профилями не смогут войти.

- **Пользователь получил сообщение, что учетная запись настроена, чтобы предотвратить вход пользователя на рабочую станцию.** Пользователь пытается обратиться к компьютеру, который не был определен как рабочая станция входа в систему. Если пользователь имел доступ к этой рабочей станции, то измените для нее информацию о входе (см. раздел «Настройка компьютеров, с которых пользователи входят в систему»).

Часть III

Управление данными в Microsoft Windows 2000

Третья часть книги посвящена управлению данными в Microsoft Windows 2000. Глава 10 начинается с объяснения процедуры добавления жестких дисков в систему и разбивки их на разделы. Затем обсуждаются такие общие задачи организации файловых систем и дисков, как дефрагментация дисков и шифрование данных. В главе 11 рассматриваются средства управления наборами томов и RAID-массивами, а также восстановление поврежденных массивов. В главе 12 речь идет об управлении файлами и каталогами. В главе 13 вы узнаете, как открыть совместный доступ к файлу, диску или папке для пользователей удаленной сети и Интернета. Глава 14 посвящена архивации и восстановлению данных и объясняет, как организовать пул носителей.



Глава 10

Управление файловыми системами и дисками

Жесткий диск — самое распространенное устройство хранения данных на сетевых рабочих станциях и серверах. Пользователи нуждаются в жестких дисках, чтобы хранить текстовые документы, электронные таблицы и другие типы данных. Диски организованы в файловые системы, к которым пользователи могут обращаться как локально, так и удаленно.

- Локальные файловые системы устанавливаются на компьютере пользователя и не требуют для доступа удаленных сетевых соединений. Пример локальной файловой системы — диск С, доступный на большинстве рабочих станций и серверов Вы обращаетесь к диску С, используя путь С:\.
- Удаленная файловая система доступна через сетевое соединение с удаленным ресурсом. Вы можете подключиться к удаленной файловой системе через функцию проводника Map Network Drive (Подключить сетевой диск).

Где бы ни были расположены дисковые ресурсы, администратору системы нужно управлять ими. Здесь обсуждаются средства и методики управления файловыми системами и дисками. В главе 11 мы рассмотрим наборы томов и отказоустойчивость. В главе 12 рассказывается об управлении файлами и каталогами

Добавление жестких дисков

Прежде чем вы откроете клиентам доступ к жесткому диску, надо сконфигурировать его и выбрать способ его использования. Microsoft Windows 2000 позволяет по-разному кон-

фигурировать жесткий диск. Выбор методики зависит от типа данных, с которыми вы работаете, и требований сетевой среды. Для универсальной пользовательской информации на рабочей станции можно сконфигурировать отдельные диски как автономные устройства хранения данных. Тогда пользовательская информация хранится на жестком диске рабочей станции, где к ней можно обращаться локально.

Хранить данные на одном диске удобно, но не надежно. Для повышения надежности и производительности можно объединить несколько дисков. Windows 2000 поддерживает наборы дисков и встроенную технологию RAID-массивов. RAID-массивы обычно устанавливают на серверы Windows 2000, а не па рабочие станции.

Физические диски

Независимо от того, что вы используете — отдельные диски или наборы, вам нужны физические диски — аппаратные устройства хранения данных. Объем информации, который можно хранить на диске, зависит от его размера и применения сжатия. Объем типичных дисков сейчас — 2-40 Гб. С Windows 2000 обычно применяются два типа дисководов: SCSI и IDE.

Термины SCSI и IDE определяют тип интерфейса жесткого диска, применяемый для связи с контроллером диска. SCSI-диски используют SCSI-контроллеры, а IDE-диски — IDE-контроллеры. Вообще SCSI-диски дороже, чем IDE, но быстрее и обладают более широкими возможностями.

Примечание Вы увидите большое количество аббревиатур, связанных с дисками IDE и SCSI. Пусть они вас не смущают. В отношении SCSI-дисков часто говорят об Ultra SCSI, Wide SCSI, SCSI-2 и SCSI-3. Стандарты SCSI-2 и SCSI-3 — последователи оригинальной спецификации SCSI. Эти новые версии используют интерфейсы Ultra или Wide SCSI и обладают более высокой скоростью в сравнении с обычным интерфейсом SCSI. С другой стороны, EIDE — усовершенствованная версия IDE, которая также быстрее обычного IDE. Одна из самых современных спецификаций EIDE — Ultra DMA (ATA-4). Забавно, но обозначения EIDE, Ultra DMA, и Ultra ATA могут относиться к одному типу дисководов. Мы обсудим стандартные интерфейсы SCSI и IDE.

SCSI-диски

SCSI позволяет подключить до 7 дисков к одному контроллеру. Каждому диску, подключенному к первичному контроллеру, присваивается числовой код от 0 до 6 — SCSI ID (идентификатор) диска, означающий, что диск 0 — это SCSI ID O, диск 1 — SCSI ID 1 и т. д. Контроллеру самого диска обычно назначается SCSI ID 7. Диски на вторичных контроллерах обозначаются номерами, следующими за последним занятым номером первичного контроллера. Так, если на первом контроллере семь дисков, то у первого диска на втором контроллере будет SCSI ID 8.

Обычно SCSI ID присваивается диску перед его установкой с помощью перемычек на его торце. Вместо перемычек на некоторых дисках есть кнопка или аналогичный механизм для настройки SCSI ID. Чтобы изменить идентификатор, нужно выключить диск и затем включить снова. Это гарантирует вступление изменений в силу.

SCSI-устройства подключаются к контроллеру последовательно одно за другим. Первое и последнее устройство в цепочке должны быть правильно терминированы. Как правило, SCSI-контроллер сам терминирует первое устройство, а фактически устанавливать терминатор (специальный резистор) приходится лишь на последнее устройство в цепочке.

Жесткий диск необходимо форматировать на низком уровне. Обычно изготовители сами форматируют SCSI-диски. Если вам потребуется провести низкоуровневое форматирование на месте, используйте служебную программу изготовителя.

IDE-диски

К IDE-контроллеру можно подключить до двух дисков. Диску, подключенному к первичному контроллеру, присваивают номер 0 (для первого ;,иска) или 1 (для второго). Диски на вторичных контроллерах обозначаются номерами, следующими за последним занятым номером первичного контроллера. Например, если на первом контроллере два диска, то первый диск на втором контроллере получит номер 3.

Как и со SCSI-дисками, номер IDE-диску присваивается перед установкой. Если это первый IDE-диск на контроллере, нужно сделать его главным. Если на контроллере два диска, установите один диск как главный, а другой — как подчиненный.

Вообще при установке нового диска, существующий диск становится главным, а новый — подчиненным.

Примечание Вы не сможете отформатировать IDE-диск на низком уровне — это делает его изготовитель.

Подготовка диска к работе

Установленный диск необходимо сконфигурировать, разбив на разделы и создав в них файловые системы. Раздел — это область физического диска, которая функционирует как отдельное устройство. Создав раздел, можно создать на нем файловую систему.

Использование консоли Disk Management

Для конфигурации дисков служит оснастка Disk Management (Управление дисками). Она облегчает работу с внутренними и внешними дисками на локальной или удаленной системе. Disk Management запускается так.

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирвоание) и щелкните ярлык Computer Management (Управление компьютером).
2. Вы автоматически подключитесь к локальному компьютеру, на котором запускается консоль Computer Management. Для управления жесткими дисками другого компьютера в дереве консоли щелкните правой кнопкой Computer Management и выберите в контекстном меню команду Connect To Another Computer (Подключиться к другому компьютеру). Затем выберите систему, дисками которой вы хотите управлять.

Совет Если диспетчер логических дисков выдал сообщение об ошибке, прочтите его и щелкните OK. Невозможность подключиться к службе диспетчера логических дисков обычно означает, что эта служба или связанные административные службы не запущены на локальной или удаленной системе. При необходимости запустите службы Logical Disk Manager {Диспечтер логических дисков) и Logical Disk Manager Administrative Service (Служба администрирования диспетчера логических дисков), как было описано в главе 3. Сетевые политики и доверия также могут влиять на возможность удаленно управлять компьютерами.

3. В консоли Computer Management раскройте узел Storage (Запоминающие устройства) и щелкните Disk Management.

Теперь вы можете управлять дисками на локальной или удаленной системе.

Оснастка Disk Management обладает тремя представлениями: список томов, графический вид и список дисков.

Примечание Созданный, но не отформатированный раздел считается свободным местом. Если часть диска не относится к какому-то разделу, она считается неразмеченной.

Ниже список томов представлен справа вверху, а графический вид — справа внизу (рис. 10-1).

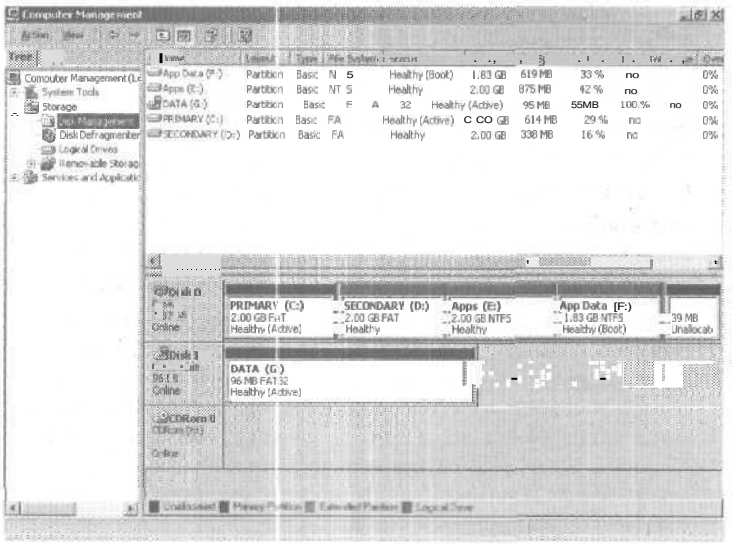


Рис. 10-1. По умолчанию в оснастке Disk Management верхний вид дает подробную информацию обо всех дисках компьютера, а нижний — обзор тех жз дисков.

Это стандартная конфигурация. Вы вправе изменить вид верхней или нижней области окна:

- чтобы изменить верхний вид, в меню View (Вид) выберите (Top) Верх, а затем — желаемый аид;
- чтобы изменять нижний вид, в меню View выберите Bottom (Низ), а затем — желаемый вид;
- чтобы скрыть нижний вид, в меню View выберите Bottom, а затем — Hidden (Скрыть).

Вид списка томов

В Disk Management вид списка томов дает подробную информацию обо всех дисках на компьютере. Щелчок названия столбца, например Volume (Том), позволяет сортировать информацию о дисках в этом столбце. Названия столбцов:

- **Volume** (Том) — буква диска и название тома, например (C:);
- **Layout** (Расположение) — расположение диска, например раздел или том;
- **Type** (Тип) — тип диска, например базовый или динамический;
- **File** System (Файловая система) — тип файловой системы, например FAT (таблица размещения файлов), FAT32 или NTFS (файловая система Windows NT);
- Status (Состояние) — состояние тома, например исправен или неисправен;
- **Capacity** (Емкость) — объем данных, который может содержаться в томе;
- **Free Space** (Свободно) — объем свободного места в мегабайтах;
- % Free (Свободно %) — объем свободного места в процентах от полной емкости диска;
- **Fault Tolerance** (Отказоустойчивость) — использует ли диск отказоустойчивые возможности Windows 2000, например зеркальное отображение или чередование;
- **Overhead** (Накладные расходы) — суммарный дополнительный объем диска, требуемый для работы функций отказоустойчивости.

Примечание Наборы томов и отказоустойчивость обсуждаются в главе 11.

Графический вид

В оснастке Disk Management графический вид позволяет просмотреть все установленные на системе физические и логические диски. В нашем примере три дисковых устройства: диск 0, несъемный диск емкостью 7,87 Гб, диск 1 - съемный и CDRom 0 — привод CD-ROM. Диск 0 дополнительно разбит на разделы: основной, три логических диска и свободная часть диска. Для этих разделов диска даны следующие сведения: буква диска, метка раздела или тома, тип

файловой системы, например FAT, FAT32 или NTFS, размер раздела диска в мегабайтах, а также состояние разделов или томов, например, исправны они или нет.

Резюмирующая информация для физических дисковых устройств включает номер диска и тип устройства (основной, съемный или CD-ROM), емкость диска и состояние устройства, т. е. доступно оно или нет.

Вид списка дисков

В оснастке Disk Management вид списка дисков резюмирует сведения о физических дисках. Эта информация включает номер диска и его тип (основной, съемный или CD-ROM), емкость диска, объем неразмеченной части (если она есть), состояние дискового устройства (доступно оно или нет) и тип интерфейса (IDE или SCSI).

Более подробная информация о **дисках**

Из окна Disk Management можно получить и более подробную информацию по разделу диска, щелкнув его правой кнопкой, а затем выбрав в контекстном меню команду Proper-

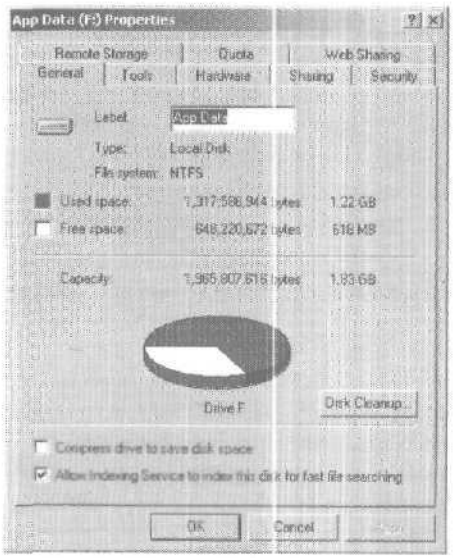


Рис. 10-2. Вкладка Gereral окна свойств содержит подробную информацию о диске.

ties (Свойства). Вы увидите то же диалоговое окно (рис. 10-2). что открывается из Windows Explorer (после открытия окна свойств диска). На вкладке General (Общие) окна свойств отображается:

- буква лиска для раздела;
- текстовая метка раздела (называемая меткой тома);
- тип диска: локальный диск — диск текущей компьютерной системы, сетевой — диск на удаленной системе, доступный по сетевому подключению (также есть типы для флоппи-дисковода, привода CD-ROM и ОЗУ-дисков);
- тип файловой системы, например FAT, FAT32 или NTFS;
- объем занятого места на диске;
- объем свободного места на диске;
- суммарная емкость диска.

Установка и проверка нового диска

Горячая замена — возможность удалять устройство без выключения компьютера. Как правило, диски с поддержкой горячей замены устанавливаются и удаляются с передней панели компьютера. Если ваш компьютер поддерживает горячую замену дисков, вы можете установить диски на компьютер, не выключая его. Затем в оснастке Disk Management и в меню Action (Действие) выберите Rescan Disks (Повторить сканирование дисков): новые диски будут добавлены как базовые. Если установленный диск не найден, попробуйте перезагрузить компьютер.

Если компьютер не поддерживает горячую замену дисков, выключите его, а потом установите новые диски. Затем выполните команду Rescan Disks, как описано выше.

Состояниедиска

Знать состояния диска полезно при установке нового диска и при устранении проблем. Disk Management отображает состояние диска в списке томов и в графическом виде (табл. 10-1).

Табл. 10-1. Основные значения состояния диска и их расшифровка.

Состояние	Описание	Решение
Online (Подключен)	Нормальное состояние диска. Оно означает, что диск доступен и не имеет	Известных проблем на диске не обнаружено.

Табл. 10-1. *(продолжение)*

Состояние	Описание	Решение
	ошибок. Все, как базовые, так и динамические диски отображают это состояние.	
Online (Errors) [Работает (ошибки)]	На динамическом диске обнаружены ошибки ввода-вывода.	Попробуйте устранить временные ошибки, выбрав команду Reactivate Disk (Реактивизировать диск).
Offline **(Но** подключен)	Динамический диск недоступен и может быть поврежден, либо доступ к нему временно невозможен. Если имя диска изменилось на Missing, то этот диск больше не может размещаться или идентифицироваться в системе.	Проверьте диск, его контроллер и шлейфы на наличие ошибок. Убедитесь, что диск подсоединен к питанию и соответствующим образом подключен. Команда Reactivate Disk позволяет снова (если это возможно) включить диск.
Foreign (Чужой)	Динамический диск подключен к компьютеру, но не импортирован. Включенный после сбоя диск иногда может обозначаться как Foreign.	Для добавления диска в систему служит команда IMPORT FOREIGN DISKS (импорт чужих дисков).
Unreadable (Не читается)	Диск временно недоступен. Это может быть вызвано повторным поиском дисков. Как базовые, так и динамические диски отображают это состояние.	Диски не просматриваются по причине повреждения или наличия ошибок ввода-вывода. Команда RESCAN DISK позволяет исправить (по возможности) ошибку. Можно также перезагрузить систему.
Unrecognized (Неопознан)	Диск неизвестного типа и не может использоваться системой. *Так* может отображаться диск другой системы (не-Windows).	Диск нельзя использовать на компьютере. Попробуйте другой диск.
No Media (Нет носителя)	Ничего не было установлено в CD-ROM или съемный диск. Только CD-ROM и съемные диски отображают это состояние.	Для включения вставьте компакт-диск, дискету или съемный диск.

Базовые и динамические диски

Windows 2000 поддерживает два типа дисковых конфигураций.

- **Базовая** Стандартный дисковый тип, используемый в предыдущих версиях Windows. Базовые диски разбиваются на разделы и могут применяться с предыдущими версиями Windows.
- **Динамическая** Усовершенствованный дисковый тип для Windows 2000, обновляемый (в большинстве случаев) без перезагрузки. Динамические диски делятся на тома и применяются только с Windows 2000.

Использование базовых и динамических дисков

При обновлении системы до Windows 2000 диски с разделами распознаются как базовые. А при установке Windows 2000 на новую систему с неразбитыми на разделы дисками можно назначить их базовыми или динамическими.

Базовые диски поддерживают все отказоустойчивые возможности Windows NT 4.0. Можно использовать базовые диски для поддержания или удаления существующих конфигураций управления, зеркального отображения и чередования. Однако базовый тип не позволяет создавать отказоустойчивые диски; для этого их надо преобразовать в динамические, а затем создать тома, использующие зеркальное отображение и чередование. Отказоустойчивость и возможность модифицировать диски без перезагрузки — ключевые характеристики, отличающие базовые и динамические диски. Прочие доступные характеристики зависят от форматирования диска.

На одном компьютере можно задействовать как базовые, так и динамические диски; главное, чтобы том содержал диски одинаковых типов. Например, диски C и D, созданные под Windows NT 4.0 с применением зеркального отображения, можно использовать под Windows 2000. Изменяя тип диска C па динамический, надо модифицировать и диск D. Об изменении типа диска с базового на динамический см. раздел «Изменение типов дисков».

Особенности базовых и динамических дисков

Работая с базовыми или динамическими дисками, помните о специальных дисковых разделах.

- **Системный** раздел/том содержит файлы, специфичные для оборудования и необходимые для загрузки ОС. В компьютерах на базе процессора Alpha системный раздел (том) должен иметь формат FAT. Системный раздел не может быть частью составного тома, массива RAID-5 или тома с чередованием.
- **Загрузочный** раздел/том содержит ОС и файлы поддержки. Системная и загрузочная области могут располагаться на одном разделе.
- **Активный** раздел/том — область диска, с которой запускается компьютер. Если на компьютере несколько ОС, активный диск должен содержать загрузочные файлы для всех из них. Он также должен быть первичным разделом на базовом диске. Если па компьютере только Windows 2000, активный диск должен быть простым томом на динамическом диске (может совмещаться с системным).

Создание активного раздела

Чтобы выбрать активный раздел, сделайте так.

1. Убедитесь, что загрузочные файлы находятся на первичном разделе диска, который будет активным. Для Windows NT/2000 эти файлы: BOOT.INI, NTDETECT.COM, NTLDR и BOOTSECT.DOS. Также может потребоваться NTBOOTDD.SYS.
2. Запустите консоль Disk Management.
3. Щелкните правой кнопкой раздел, который хотите сделать активным, и выберите Mark Partition Active (Сделать раздел активным).

Примечание Нельзя помечать активным том: при преобразовании базового диска, содержащего активный раздел, в динамический диск этот раздел становится простым томом, который затем автоматически становится активным.

Изменение типов дисков

Базовые диски предназначены для применения с предыдущими версиями Windows. Динамические диски позволяют задействовать новейшие преимущества Windows 2000. Их нельзя использовать с предыдущими версиями Windows, зато они работают с другими ОС, например с Unix, после создания отдельного тома для прочих (не-Windows) систем. Ди-

намические диски нельзя применять в переносных компьютерах.

Windows 2000 предоставляет средства для трансформации базового лиска в динамический и обратно. При этом разделы автоматически преобразуются в тома соответствующего типа. Тома уже нельзя преобразовать в разделы. Для этого нужно удалить тома на динамическом диске, а затем изменить тип диска обратно на базовый. Удаление тома уничтожает всю информацию на диске.

Преобразование базового диска в динамический

Перед изменением типа диска с базового на динамический убедитесь, что, во-первых, диск не будет использоваться со старыми версиями Windows, во-вторых, в конце диска есть 1 Мб свободного места. Хотя Disk Management автоматически резервирует это место при создании разделов и томов, инструментам управления дисками других ОС это может не требоваться. В итоге преобразовать диск не удастся. Перед преобразованием учтите также следующее.

- Нельзя модифицировать диски с размером сектора больше 512 байт, а если он больше, сначала переформатируйте диск.
- Нельзя преобразовывать съемные диски в динамический тип. Можно лишь конфигурировать дисковод съемных дисков как базовый диск с первичными разделами.
- Нельзя модифицировать диск, если системный или загрузочный раздел является частью составного тома, RAID-5 или тома с чередованием, поэтому перед преобразованием нужно удалить эти функции.
- Можно модифицировать диски с разделами других типов, которые являются частью составного тома, RAID-5 или тома с чередованием. Эти тома становятся динамическими томами соответствующего типа. Однако при этом диски в наборе надо модифицировать все вместе.

Базовый диск преобразуется в динамический так.

1. В консоли Disk Management в списке дисков или в левой части окна диаграмм щелкните правой кнопкой базовый диск, который нужно преобразовать. Затем выберите Upgrade To Dynamic Disk (Обновление до динамического диска).

2. В окне Upgrade To Dynamic Disk отметьте диски, которые нужно модифицировать. При преобразовании составных томов, массивов RAID-5 или томов с чередованием, убедитесь, что вы выбрали все диски в наборе, так как их нужно модифицировать все вместе. Щелкните OK.
3. В диалоговом окне Disks To Upgrade представлены модифицируемые диски (рис. 10-3). Кнопки и колонки диалогового окна содержат следующую информацию:
   - **Name** (Имя) — номер диска;
   - **Disk Contents** (Диск содержит) — тип и состояние разделов; загрузочный, активный, используется и т. п.
   - **Will Upgrade** (Будет обновлен) — определяет, будет ли диск модифицирован. Если диск не отвечает условиям, он не будет преобразован, и надо произвести его коррекцию (как описано выше).
   - **Details** (Сведения) — отображает тома выбранного диска.
   - **Upgrade** (Обновить) — начинает операцию преобразования.

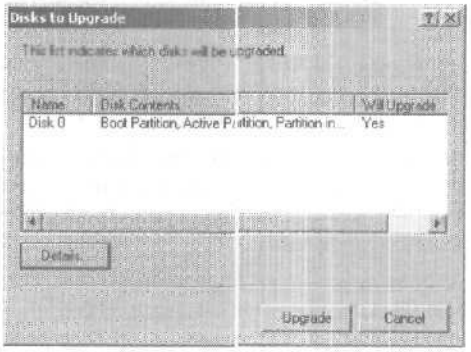


Рис. 10-3. Перед продолжением обратите внимание на колонки Disk Contents и Will Upgrade.

4. Если все готово для преобразования, щелкните Upgrade. Disk Management предупредит вас, что преобразовав диск, вы больше не сможете загружать предыдущие версии Windows с томов выбранных дисков. Щелкните Yes (Да).
5. Disk Management перезагрузит систему, если выбранный диск содержит загрузочный, системный или используемый раздел.

Обратное преобразование динамического диска в базовый

Перед обратным преобразованием нужно удалить с диска все динамические тома. Как только вы это сделали, щелкните диск правой кнопкой и выберите Revert To Basic Disk (Восстановить конфигурацию базового диска). Эта операция преобразует динамический диск в базовый, после чего можно будет создать новые разделы и логические диски.

Реактивация динамических дисков

Если состояние динамического диска отображается как Online (Errors) или Offline, зачастую, чтобы устранить проблему, нужно просто реактивизировать диск.

1. В оснастке Disk Management щелкните правой кнопкой динамический диск, который надо реактивизировать, и выберите Reactivate Disk (Реактивизировать диск). Подтвердите действие при запросе.
2. Если состояние диска не изменилось, перезагрузите компьютер. Если это не помогло, проверьте дисковод, контроллер и шлейфы на наличие ошибок, также убедитесь, что дисковод правильно подсоединен и подключен к питанию.

Повторное сканирование дисков

Повторное сканирование всех дисков системы обновляет конфигурацию дисководов компьютера. Иногда это может решить проблемы дисков, которые отображаются как Unreadable. В результате повторного сканирования конфигурация дисков может измениться, поэтому нужно внести изменения в файл BOOT.INI (см. раздел «Обновление загрузочного диска»).

Повторное сканирование дисков системы осуществляется в оснастке Disk Management из меню Action (Действие) командой Rescan Disk (Повторить сканирование дисков).

Совет Для дополнительной проверки проведенных изменений сделайте снимок экрана конфигурации дисков в Disk Management до и после сканирования. Типичная конфигурация моего сервера: флоппи-дисковод A, логические диски C, D, E, и F, съемный диск G и CD-ROM H. После повторного сканирования съемный диск был B, в результате чего количество загрузочных разделов изменилось (Windows 2000 не выдала по этому поводу предупреждений).

При перезагрузке Windows 2000 некорректно заявляет, что файл NTOSKRNL.EXE в корневой папке Windows 2000 нуждается в восстановлении. Используя аварийный загрузочный диск (о его создании см. главу 14), можно изменить файл BOOT.INI и восстановить систему. Без аварийного диска реставрировать установку Windows 2000 можно с установочных дисков Windows 2000 (об их создании см. также главу 14).

Перенос динамического диска в новую систему

Задача присоединения дисков **к системе в Windows** 2000 решается **очень просто.**

1. Запустите Disk Management на системе с установленными динамическими дисками.
2. Проверьте состояние дисков и убедитесь, что диск опознается как исправный. Иначе перед подключением нужно восстановить поврежденные разделы и тома,
3. Удалите букву диска и путь доступа к диску (см. раздел «Назначение буквы и пути диска»).
4. Если диск и обе системы поддерживают функцию горячей замены, просто извлеките диск с одного компьютера и переставьте его в другой. Иначе выключите компьютеры и переставьте диски со старого компьютера на новый, а затем вновь включите компьютер.
5. На компьютере, куда устанавливаются диски, в меню Action выберите Rescan Disks. Когда сканирование дисков кончится, щелкните правой кнопкой диск, отображаемый как Foreign, и в контекстном меню выберите Import Foreign Disks.

Использование базовых дисков и разделов

При установке нового компьютера или модернизации старого часто требуется разбить его диски на разделы. Это можно сделать из консоли Disk Management. Если вам нужно с одного компьютера загружать Windows 95/98 или Windows NT/2000, создайте для каждой ОС свой раздел.

Внимание! Перед какими-либо изменениями на жестком диске проанализируйте возможные последствия. Изменение информации о разделах дисков может привести к потере

данных, а неправильная конфигурация разделов может вообще помешать загрузке системы. Во избежание проблем с конфигурацией Windows 2000 ограничивает операции над системными и загрузочными разделами.

Понятие о разделах диска

Windows **2000** использует **два** типа разделов: основные и дополнительные.

- Основные разделы — части диска, куда можно сохранить файлы. Физический диск может содержать до четырех основных разделоп. Для доступа пользователей к основному разделу нужно создать на нем файловую систему.
- В отличие от основных разделов к дополнительному нельзя обращаться напрямую. Вместо *этот* можно создать на дополнительном разделе один и более логических дисков, на которых будут храниться файлы. Разбивка дополнительного раздела на логические диски позволяет разделить физический диск более чем на четыре части.

В Windows 2000 физический диск может содержать до четырех основных разделов и/или один дополнительный. Это допускает дна варианта конфигурации дисков: первый — от 1 до 4 основных дисков, второй — от 1 до 3 основных и 1 дополнительный.

Примечание В MS-DOS физический диск может состоять только из одного основного раздела — загрузочного. Если планируется загрузка Windows 2000 из MS-DOS, создайте один основной раздел, а добавочные логические диски создайте в дополнительном разделе.

Назначение **букв** дискам

После разбиения диска надо отформатировать разделы, чтобы назначить буквы дисков. Это высокоуровневое форматирование, создающее структуру файловой системы в отличие от низкоуровневого форматирования, которое подготавливает диск к работе.

Вам, вероятно, знаком диск С, используемый в Windows 2000. Так вот, диск С — это просто указатель на раздел диска. Если диск разбивается на несколько разделов, то каждому из них присваивается своя буква. Буквы дисков служат для доступа к файловым системам разделов физического диска.

В отличие от MS-DOS, где буквы дискам назначаются автоматически, начиная с C, Windows 2000 позволяет определять их самостоятельно (доступны все буквы от C до Z).

Примечание Буква A обычно резервируется для системного флоппи-дисковода. Если в системе установлен второй флоппи-дисковод, ему присваивается буква B, поэтому у вас в распоряжении буквы от C до Z. Не забудьте, что для CD-ROM, ZIP-дисководов и других типов носителей также требуются буквы. Одновременно можно использовать до 24 букв. Если не хватает томов, можно смонтировать их, используя путь к диску.

Назначение путей к **диску**

В Windows NT 4.0 активных томов может быть не более 24. Windows 2000 обходит это ограничение, позволяя монтировать диски, используя пути, которые определяются как местоположение папки на другом диске. Например, можно смонтировать дополнительные диски, ссылающиеся на папки E:\data1, E:\data2 и E:\data3.

Пути к дискам применимы как на основных, так и на динамических дисках. Единственное ограничение: вы можете монтировать их только *на* пустые папки на NTFS-дисках.

Цветовая маркировка разделов

Для наглядности Disk Management маркирует основные и дополнительные разделы (с логическими дисками) разными цветами. Например, основные разделы могут быть кодированы темно-синей полосой, а логические диски на дополнительных разделах — светло-голубой. Легенда цветовой схемы расположена внизу окна Disk Management. Цвета можно изменить Б диалоговом окне View Settings (Просмотр параметров) в меню View/Settings (Вид/Параметры).

Создание разделов и логических дисков

Разделы и логические лиски создаются в консоли Disk Management,

1. В графическом виде оснастки Disk Management щелкните правой кнопкой область, помеченную Unallocated Space (Незанятое место), и выберите Create Partition (Создать раздел). Запустится мастер Create Partition (Мастер со-

здания разделов). В первом окне мастера щелкните **Next (Далее). Теперь** можно **выбрать тип** раздела **(рис.** 10-4).

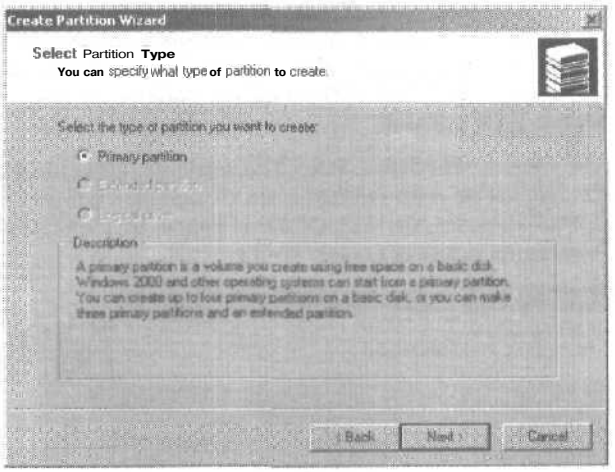


Рис 10-4. В мастере Create Partition выберите тип раздела и щелкните Next.

2. Чтобы создать основной раздел, выберите Primary Partition (Основной раздел). Каждый физический диск может содержать до 4 основных разделов. Основной раздел может занимать либо весь диск, либо его размер корректируют в соответствии с конфигурацией рабочей станции или сервера.
3. Чтобы создать дополнительный раздел, выберите Extended Partition (Дополнительный раздел). Физический диск может содержать один дополнительный раздел, который может состоять из нескольких логических дисков (областей раздела со своей файловой системой).

Примечание Если на диске уже есть дополнительный раздел, этот вариант будет недоступен. Удалите существующий раздел и создайте новый, что приведет к потере всех данных. На съемных дисках можно создавать только основные разделы.

4. Чтобы создать логический диск вне дополнительного раздела, выберите Logical Drive (Логический диск).

Совет Можно как угодно изменять размер логических дисков, но при этом учитывать их назначение на данной рабочей станции или сервере. В общем случае логические диски применяются для деления большого диска на управляемые разделы. С этой точки зрения может понадобиться разбить диск емкостью 21 Гб на три логических диска емкостью 7 Гб каждый.

5. В окне Specify Partition Size (Указание размера раздела) определяется максимальный и минимальный размер раздела в Мб в поле Amount Of Disk Space To Use (Размер создаваемого раздела) (рис. 10-5).

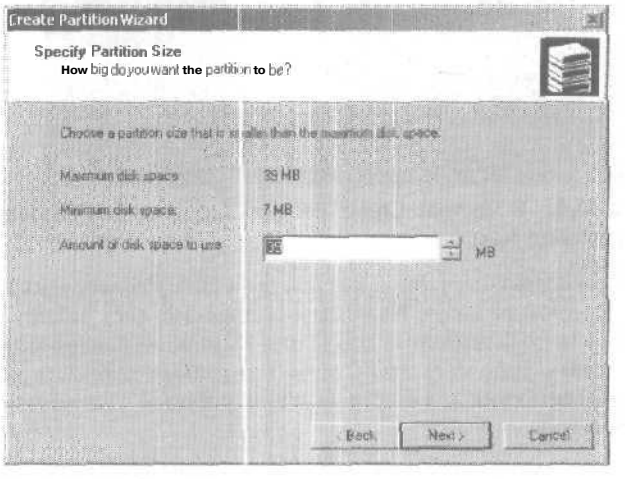


Рис. 10-5. Задайте размер основного раздела между максимальным и минимальным значениями, затем щелкните Next.

6. Чтобы назначить букву диска или путь, нужно выбрать один из следующих параметров:
   - Assign **A Drive Letter** позволяет назначить букву диска: выберите в списке доступную букву;
   - **Mount** This Volume **To An Empty Folder** That **Supports Drive Paths** позволяет назначить путь к диску: наберите путь к существующей панке или щелкните Browse (Обзор), чтобы найти или создать папку;
   - **Do Not Assign A Drive Letter Or Drive Path** позволяет не назначать букву и путь к диску, при необходимо это можно сделать позже.

7. В окне Format Partition (Форматирование раздела) укажите, форматировать ли раздел (рис. 10-6). При форматировании следуйте инструкциям из раздела «Форматирование разделов».

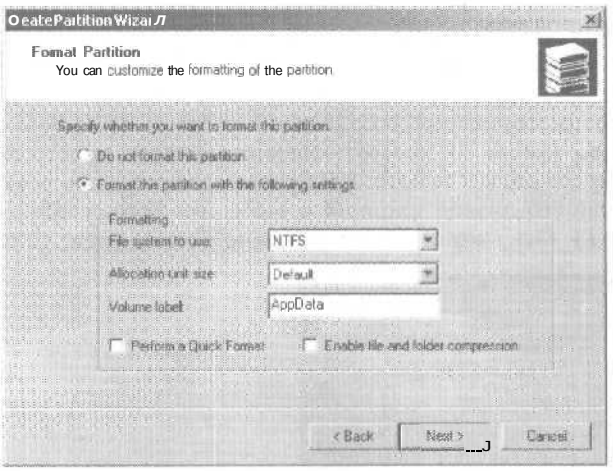


Рис. 10-6. Отформатируйте раздел, указав файловую систему и метку тома.

8. Щелкните Next, а затем Finish (Готово). При добавлении разделов на физический диск, содержащий Windows 2000, можно по неосторожности изменить количество загрузочных разделов. Тогда Windows 2000 выдаст предупреждение, что количество загрузочных разделов изменилось (рис. 10-7). Щелкните Yes (Да).

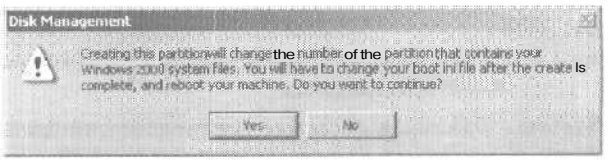


Рис. 10-7. При модификации физического диска, содержащего ОС, может потребоваться изменить файл BOOT.INI.

9. Затем Disk Management создаст раздел, назначит букву или путь к диску (по выбору) и отформатирует раздел (по выбору). Если до этого отображалось предупреждение,

появится новое, предлагающее изменить файл BOOT.INI. Внесите соответствующие изменения в файл BOOT.INI, поменяйте указатель на загрузочный раздел (см. раздел «Обновление загрузочного диска») и перезагрузите систему.

Форматирование разделов

Форматирование создает на разделе файловую систему и удаляет всю существующую информацию. Это высокоуровневое форматирование, создающее структуру файловой системы, в отличие от низкоуровневого, которое просто подготавливает диск к работе. Чтобы отформатировать раздел, щелкните его правой кнопкой и выберите Format (Форматировать). Откроется диалоговое окно Format (рис. 10-8).

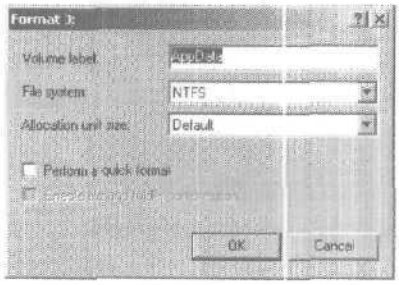


Рис. 10-8. Отформатируйте раздел, назначив ему файловую систему и метку тома.

Сравнив рис. 10-6 и 10-8, вы увидите, что доступные поля абсолютно одинаковы. Поэтому для форматирования диска с помощью мастера Create Partition или диалогового окна Format используются одинаковые методы. Ниже описаны поля этого окна.

- **Volume Label** (Метка тома) определяет текстовую метку раздела, т. е. имя тома раздела.
- File **System** (Файловая система) определяет тип файловой системы, например FAT, FAT32 или NTFS. FAT — тип файловой системы, поддерживаемый MS-DOS, Windows 3.1/95/98. NTFS — тип файловой системы для Windows NT и Windows 2000. Об NTSF см. главу 12.
- **Allocation Unit Size** (Размер кластера) определяет размер кластера файловой системы — основной единицы деления дискового пространства. По умолчанию размер

кластера определяется по размеру тома и задается до форматирования. Чтобы изменить это, можно задать свой размер кластера. При использовании большого количества небольших файлов может потребоваться уменьшить размер кластера, например до 512 или 1 024 байт, тогда они будут занимать меньше места на диске.

Совет Файловые системы FAT или FAT32 можно преобразовать в NTFS с помощью служебной программы Convert, но обратно преобразовать NTFS-разделы в FAT нельзя. Обычно загрузочный раздел форматируют в системе FAT, а остальные — в NTFS. Зачастую удачным решением для систем на базе Intel x86 является применение FAT на системных разделах. Это позволяет при необходимости загружать MS-DOS.

В системах на базе RISC-процессоров NTFS не применяется. Загрузочный раздел должен иметь формат FAT. О создании разделов см. раздел «Понятие о разделах диска».

- Perform A Quick Format (Быстрое форматирование) форматирует диск, не проверяя раздел на наличие ошибок. При работе с большими разделами этот параметр может сэкономить несколько минут. Но все же рекомендуется проверять диск на наличие ошибок, гак как при этом Disk Management отмечает и блокирует поврежденные сектора.
- **Enable File And Folder Compression** (Применять сжатие файлов и папок) включает сжатие диска. Встроенная система сжатия доступна только для NTFS. Для пользователей механизм сжатия прозрачен, так как доступ к сжатым данным идентичен доступу к обычным. После выбора этого параметра файлы и каталоги на диске автоматически сжимаются. Подробнее о сжатых дисках, файлах и каталогах см. раздел «Сжатые диски и данные».

Когда будете готовы продолжать, щелкните OK. Форматирование раздела уничтожит всю информацию, поэтому Disk Management предоставит последнюю возможность прервать операцию. Щелкните OK, чтобы начать форматирование. Disk Management изменит состояние диска, отражая процедуру форматирования и процент выполнения операции. По завершении форматирования состояние диска соответственно изменится.

Обновление загрузочного диска

При добавлении разделов на диск, содержащий Windows 2000, число загрузочных разделов может измениться. Если это произошло, нужно внести соответствующие изменения в системный файл BOOT.INI (обычно расположенный на диске C).

Файл BOOT.INI содержит примерно такие строки:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(3)\WIN2000
[operating systems]
multi(0)disk(0)rdisk(0)partition(3)\WIN2000="Microsoft Windows
2000 Server" /fastdetect
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Windows NT Server
Version 4.00"
roulti(0)disk(0)rdisk(0)partition(2)\WINNT="Windows NT Server
Version 4.00 [VGA mode]" /basevideo /sos
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT
Workstation Version 4.00"
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT
Workstation Version 4.00 [VGA mode]" /basevideo /sos
```

Такие строки указывают Windows NT. где искать ОС:

```
multi(0)disk(0)rdisk(0)partition(3)\WIN2000
```

Указатели этого элемента расшифровываются так.

- **multi(0)** определяет контроллер диска, в данном случае — контроллер 0. Если вторичное зеркало расположено на другом контроллере, введите его номер. Контроллеры нумеруются от 0 до 3.

Примечание Элементы файла BOOT.INI написаны в формате ARC. На SCSI-системах, не использующих SCSI BIOS, первое поле элемента — scsi(*n*), где *n* — номер контроллера.

- **disk(0)** указывает на SCSI-адаптер (в данном случае - адаптер 0). На большинстве систем этот параметр всегда равен 0. Исключение — системы с многоканальными SCSI-адаптерами, использующие синтаксис scsi(n).
- **rdisk(0)** указывает порядковый номер диска на адаптере (в данном случае — 0). SCSI-дисководы, использующие SCSI BIOS, поддерживают номера от 0 до 6. Для остальных SCSI-дисководов этот параметр всегда 0. Для IDE -

О либо 1. Обычно требуется изменить значение этого поля, поэтому убедитесь, что ввели номер диска вторичного зеркала.

- **partition(3)** указываетраздел, содержащий ОС (в данном случае — 3).

Если загрузочный раздел Windows 2000 изменился с 3 на 4, нужно изменить файл BOOT.INI (см. выше) так:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(4)\WIN2000
[operating systems]
multi(0)disk(0)rdisk(0)partition(4)\WIN2000="Microsoft Windows
2000 Server" /fastdetect
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Windows NT Server
Version 4.00"
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Windows NT Server
Version 4.00 [VGA mode]" /basevideo /sos
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT
Workstation Version 4.00"
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT
Workstation Version 4.00 [VGA mode]" /basevideo /sos
```

Управление разделами и дисками

Disk Management предлагает массу способов управления разделами и дисками. Вы можете назначать буквы дискам, удалять разделы, задавать активный раздел и т. п. Кроме того, Windows 2000 предоставляет служебные программы для выполнения таких задач, как преобразование тома в NTFS или проверка диска.

Назначение путей и букв дискам

Диски могут быть обозначены одной буквой и одним или несколькими путями, если это пути к данным па NTFS-дисках. Назначать диску букву или путь не обязательно. Диск без указателей считается несмонтированным; смонтировать его можно позже, назначив букву и путь. Перед переносом на другой компьютер диск нужно размонтировать.

Чтобы изменить букву диска или путь, в консоли Disk Management щелкните правой кнопкой нужный диск и выберите Change Drive Letter And Path (Изменение буквы диска и пути

диска). В открывшемся окне (рис. 10-9) можно сделать следующее:

- добавить путь диска — щелкните Add (Добавить), Mount In This NTFS Folder (Подключить как следующую папку NTFS), затем наберите путь к существующей папке или щелкните Browse (Обзор), чтобы найти или создать ее;
- удалить путь диска — выберите путь, щелкните Remove (Удалить), а затем Yes (Да);
- назначить букву диска — щелкните Add, затем Assign A Drive Letter (Назначить букву диска) и выберите доступную букву;
- изменить букву диска — выберите текущую букву диска и щелкните Edit (Изменить), затем Assign A Drive Letter и выберите другую букву;
- удалить букву диска — выберите текущую букву, щелкните Remove, а затем Yes.

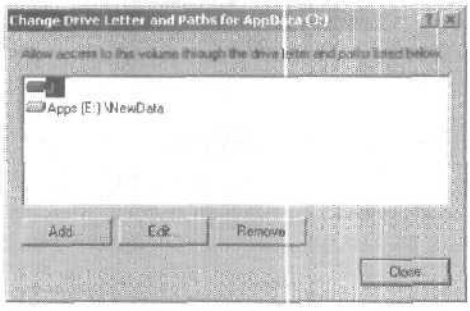


Рис. 10-9. Это окно позволяет изменить букву диска и путь.

Примечание При попытке изменить букву используемого диска Windows 2000 выдаст предупреждение. Чтобы этого избежать, выйдите из всех работающих на этом диске программ либо позвольте консоли Disk Management принудительно внести изменения, щелкнув в ответ на запрос Yes.

Изменение или удаление метки тома

Метка тома — текстовое описание диска. Метка отображается при доступе к диску из разных программ Windows 2000, например из Проводника Windows, и помогает помять, что хранится на диске. Изменять и удалять метку можно из консоли Disk Management или Проводника Windows.

Чтобы изменить или удалить метку в Disk Management или Проводнике, сделайте так,

1. Щелкните правой кнопкой раздел и выберите Properties (Свойства).
2. На вкладке General (Общие) окна свойств в поле Label (Метка) наберите новое имя или удалите метку. Щелкните OK.

Удаление разделов и дисков

Чтобы изменить конфигурацию полностью распределенного диска, может понадобиться удаление существующих разделов и логических дисков. Это ведет к уничтожению соответствующей файловой системы и потере всей информации на ней. Поэтому перед удалением сделайте резервные копии всех файлов и каталогов, содержащихся на диске.

Основной раздел или логический диск удаляется так.

1. В консоли Disk Management щелкните правой кнопкой раздел или диск, который планируете удалить, и выберите соответственно Delete Partition (Удалить раздел) или Delete Logical Drive (Удалить логический диск).
2. Подтвердите, что хотите удалить раздел, щелкнув Yes.
3. При удалении раздела физического диска, содержащего Windows 2000, количество загрузочных разделов может измениться. Если так, соответственно измените файл BOOT.INI, как было описано выше. Убедитесь, что указано новое количество используемых разделов.

Дополнительный раздел удаляется так.

1. Удалите на разделе все логические диски, как было описано выше.
2. Теперь можно выбрать область дополнительного раздела и удалить ее.

Преобразование тома в NTFS

Windows 2000 предоставляет служебную программу преобразования EAT-томов в систему NTFS — CONVERT.EXE, расположенную в папке *%SystemRoot%*. При преобразовании тома этой программой структура файлов и каталогов, а также данные сохраняются. Помните, что программы обратного преобразования (NTFS в FAT) в Windows 2000 нет. Един-

ственный способ перейти от NTFS к FAT — удалить раздел (см. предыдущий раздел), а затем создать раздел как том FAT.

Синтаксис программы преобразования

Convert — программа командной строки для преобразования диска:

convert *том* /FS:NTFS [/V]

где *том* — буква диска с двоеточием, путем диска и именем тома. Например, если нужно преобразовать диск D в систему NTFS, введите:

```
convert D: /FS:NTFS
```

Параметры и переключатели программы Convert:

- *том* — указывает рабочий том;
- /FS:NTFS — указывает, что нужно преобразовать в формат NTFS;
- /V — включает режим вывода подробных сведений.

Работа с программой Convert

Перед применением Convert проверьте, является ли раздел активным загрузочным или системным разделом, содержащим ОС. На системах Intel x86 активный загрузочный раздел можно преобразовать в NTFS. При этом система должна обладать полным доступом к разделу, что достижимо только во время запуска. Таким образом, при попытке преобразовать активный загрузочный раздел в NTFS Windows 2000 спросит, нужно ли преобразовывать диск при перезапуске. Нажав Yes, можете перезагрузить систему, запустив тем самым процесс преобразования.

Совет Обычно для полного преобразования активного загрузочного раздела требуется несколько перезагрузок. Так что не волнуйтесь и дайте системе кончить преобразование.

Системы на базе RISC-процессоров сконфигурированы на аппаратном уровне и не используют активных загрузочных разделов. Однако на RISC-компьютерах применяется системный раздел, содержащий все нужные файлы ОС. Этот раздел должен быть в файловой системе FAT, поэтому на RISC-компьютерах нельзя преобразовать системный раздел в NTFS.

Перед преобразованием диска в NTFS программа Convert проверяет наличие на нем свободного места. Вообще Convert

требуется блок свободного места размером около 25% от занятого объема. Например, если на диске 100 Мб данных, Convert потребует 25 Мб свободного места. Если свободного места не хватает, Convert прервет операцию и сообщит, что нужно освободить место на диске. Если места достаточно, Convert начнет преобразование. Придется подождать, так как процесс преобразования может занять несколько минут (или больше для объемных дисков). Не обращайтесь к файлам и приложениям на диске во время преобразования.

Проверка диска на наличие ошибок и поврежденных секторов

Служебная программа Windows 2000 для проверки целостности диска Check Disk (Проверка диска) расположена в папке *%SystemRoot%*. Check Disk (CHKDSK.EXE) служит для поиска и исправления ошибок в томах FAT, FAT32 и NTFS.

Check Disk может находить и исправлять большинство ошибок, но в первую очередь она ищет противоречие между файловой системой и связанными с ней метаданными. Один из способов проверки диска на ошибки, который реализует Check Disk, — сравнение битовой карты тома с секторами, занятыми файлами. Впрочем, возможности Check Disk ограничены. Так, она не восстанавливает поврежденные данные внутри структурно неповрежденных файлов.

Запуск Check Disk из командной строки

Check Disk можно запустить из командной строки или из других служебных программ. В режиме командной строки можно проверить целостность диска E, введя:

```
chkdsk E:
```

Для поиска и исправления ошибок на диске E служит команда:

```
chkdsk /f E:
```

Примечание Check Disk не может исправить используемые тома и спрашивает, исправить ли ошибки на диске при перезапуске.

Полный синтаксис Check Disk таков:

```
chkdsk [том[[путь]имя_файла]]] [/F] [/V] [/R] [/X] [/I] [/C]
[/L[:размер]]
```

Параметры и переключатели программы Check Disk:

- *том* — указывает рабочий том;
- *имя_файла* (только для FAT) — определяет файлы, которые нужно проверить на фрагментацию;
- /F — исправляет ошибки на диске;
- /V — в FAT/FAT32 отображает полный путь и имя каждого файла на диске, в NTFS отображает сообщения об очистке (если есть).
- /R — локализует поврежденные сектора и восстанавливает читаемую информацию (подразумевает наличие /F);
- /L:*размер* (только для NTFS) — изменяет размер файла журнала;
- /X — вынуждает сначала демонтировать том, если нужно (подразумевает наличие /F);
- /I (только для NTFS) — выполняет минимальную проверку индексных элементов;
- /C (только для NTFS) — исключает проверку циклов в структуре папок.

Удаленный запуск Check Disk

Вы можете запустить Check Disk удаленно из Проводника Windows или консоли Disk Management.

1. Щелкните правой кнопкой диск и выберите Properties (Свойства).
2. На вкладке Tools (Сервис) щелкните Check Now (Выполнить проверку).

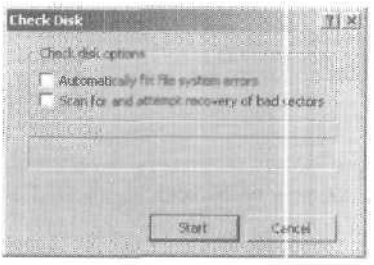


Рис. 10-10. Программа Check Disk запускается щелчком кнопки Check Now в окне свойств. Ее можно использовать для проверки диска на ошибки.

Из окна дистанционной версии Check Disk можно проверить диск на наличие ошибок, а затем и исправить их (рис. 10-10).

- Для проверки диска без исправления ошибок щелкните Start, не помечая флажки.
- Для проверки диска и исправления ошибок пометьте соответствующие флажки: исправить ошибки файловой системы, восстановить поврежденные сектора — или оба.

Дефрагментация дисков

При записи или удалении файлов данные на диске могут разбиваться на фрагменты. Когда диск фрагментирован, невозможно непрерывно записывать большие файлы на одну область диска. В результате ОС вынуждена записывать на нескольких небольших участках диска, из-за чего увеличивается время доступа к файлу при чтении. Чтобы уменьшить фрагментацию, нужно периодически анализировать и дефрагментировать диски, используя Disk Defragmenter (Дефрагментация диска).

Вот как проанализировать уровень фрагментации диска и дсфрагментировать диск.

1. В консоли Computer Management раскройте узел Storage (Запоминающие устройства) и выберите Disk Defragmenter (Дефрагментация диска).
2. Щелкните том или логический диск, с которым будете работать (рис. 10-11).
3. Для анализа уровня фрагментации раздела щелкните Analyze (Анализ). Ход процесса отображается в области Analysis Display. Фрагментированные, непрерывные и системные файлы, а также свободное место окрашены в разные цвета. Легенда с расшифровкой цветов приведена в нижней части окна. (Процесс анализа можно остановить полностью или временно.)
4. Кончив анализ, Disk Defragmenter на основании уровня фрагментации предложит соответствующее действие. Если диск сильно фрагментирован, программа предложит выполнить дефрагментацию, иначе выдаст сообщение, что Дефрагментация не требуется.
5. Чтобы начать дефрагментацию, щелкните Defragment (Дефрагментация). Ход процесса отображается в области Analysis Display. (Операцию можно остановить полностью или временно.)

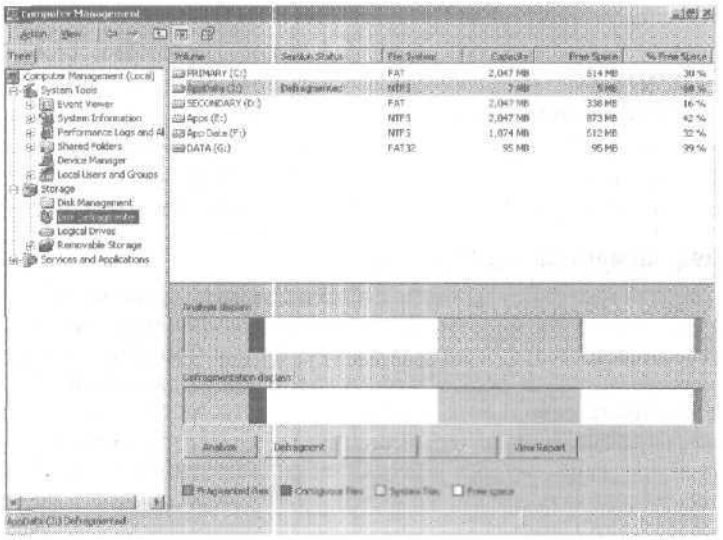


Рис. 10-11. Disk Defragmenter эффективно анализирует и дефрагментирует диски. Чем чаще изменяется информация на диске, тем чаще запускайте эту программу.

6. Щелкните View Report, чтобы просмотреть отчет об анализе или дефрагментации.

Сжатие дисков и данных

При форматировании диска в системе NTFS можно включить встроенную подсистему сжатия, которая автоматически сжимает все файлы и каталоги уже при их создании. Для пользователей эта операция незаметна, так как доступ к сжатым данным идентичен доступу к обычным. Отличие лишь в том, что на сжатом диске можно сохранить больше информации, чем на несжатом.

Сжатие каталогов и файлов

Windows 2000 позволяет избирательно сжимать каталоги/файлы. Чтобы сжать файл/каталог, сделайте так.

1. Щелкните правой кнопкой файл/каталог, который нужно сжать, и из контекстного меню выберите Properties (Свойства).
2. На вкладке General (Общие) щелкните Advanced (Другие). Выберите Compress Contents To Save Disk Space

(Сжимать содержимое для экономии места на диске) (рис. 10-12). Два раза щелкните OK.

Если каталог содержит подкаталоги, Windows 2000 выдает запрос на сжатие всех его подкаталогов — выберите Apply Changes To This Folder, Subfolders, And Files (К этой папке и ко всем вложенным файлам и папкам) и щелкните OK. Новые файлы при добавлении и копировании в сжатый каталог также автоматически сжимаются.

Примечание Несжатый файл при перемещении с другого диска сжимается. Однако при перемещении несжатого файла в сжатый каталог внутри одного NTFS-диска файл не сжимается. Имейте также в виду, что сжатый файл не может быть зашифрован.

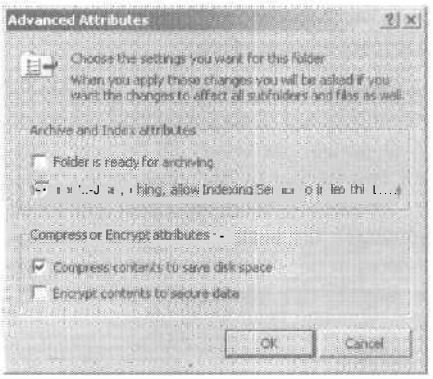


Рис. 10-12. В системе NTFS можно сжать файл или каталог, пометив флажок Compress.

Разуплотнение сжатых файлов и каталогов

Для разуплотнения файла/каталога, сделайте так,

1. Щелкните правой кнопкой файл/каталог в Проводнике Windows.
2. На вкладке General окна свойств щелкните Advanced, сбросьте флажок Compress Contents To Save Disk Space и два раза щелкните OK.

Windows 2000 отменит сжатие и разожмет файл. Windows 2000 разуплотняет все файлы в каталоге. Вы можете отменить сжатие подкаталогов: выберите в ответ на запрос Apply Changes To This Folder, Subfolders, And Files и щелкните OK.

Совет В Windows 2000 есть служебные программы командной строки: Compact (COMPACT.EXE) для сжатия информации и Expand (EXPAND.EXE) — для разуплотнения.

Шифрование дисков и данных

Windows 2000 поддерживает шифрование данных на томах NTFS. Зашифрованные файлы могут быть прочитаны только тем, кто их зашифровал. Однако их можно копировать, перемешать и переименовывать так же, как и любые другие. Эти действия не влияют на шифрование данных.

Процесс шифровки и расшифровки называется шифрованной файловой системой (Encrypting File System, EFS). Стандартная настройка EFS позволяет пользователям шифровать файлы без специального разрешения. Файлы шифруются с применением общего или закрытого ключей, автоматически генерируемых EFS для каждого пользователя.

Совет Применяемый алгоритм шифрования — расширенный стандарт шифрования данных (Data Encryption Standard, DESX), который по умолчанию реализует 56-битное шифрование. Для большей безопасности пользователи из Северной Америки могут заказать у Microsoft пакет Enhanced CryptoPAK, обеспечивающий 128-битное шифрование. Администраторы, выполняющие роль агентов восстановления шифрованных данных, вправе при необходимости расшифровать любые файлы.

Шифрование каталогов и файлов

Windows 2000 позволяет выбрать для шифрования отдельные файлы и каталоги на томах NTFS. При шифровании данные файла преобразуются в шифрованный формат, и прочитать их может только тот, кто их зашифровал. Пользователи могут шифровать файлы, если у них есть соответствующее разрешение. При шифровании папки маркируются как шифрованные, но на самом деле только файлы внутри этой папки зашифрованы. Все файлы, создаваемые и добавляемые в «зашифрованную» панку, автоматически шифруются.

Вот как зашифровать ланку/файл.

1. Щелкните правой кнопкой файл или каталог, который хотите **зашифровать,** и выберите Properties (Свойства).

2. На вкладке General окна свойств щелкните Advanced и выберите Encrypt Contents To Secure Data (Шифровать содержимое для защиты данных). Затем два раза щелкните OK.

Примечание Нельзя зашифровать сжатые и системные файлы, а также файлы, доступные только для чтения. При попытке их зашифровать сжатые файлы автоматически разуплотняются, после чего шифруются. При попытке зашифровать системные файлы выдается сообщение об ошибке.

Если каталог содержит подкаталоги, появится запрос на шифрование всех его подкаталогов: выберите Apply Changes To This Folder, Subfolders, And Files и щелкните OK.

Примечание На томах NTFS файлы при перемещении, копировании и переименовании остаются зашифрованными. Перед копированием или перемещением зашифрованного файла на диск в формате FAT или FAT32 он автоматически дешифруется. Но для такого копирования или перемещения требуется специальное разрешение.

Дешифровка файлов и каталогов

Если позже понадобится расшифровать файл/каталог, сделайте так.

1. В Проводнике Windows щелкните правой кнопкой файл или каталог.
2. На вкладке General окна свойств щелкните Advanced. Сбросьте флажок Encrypt Contents To Secure Data и два раза нажмите OK.

Отдельные файлы Windows 2000 дешифрует и сохраняет в первоначальном формате. Для каталогов Windows 2000 дешифрует все вложенные файлы. Можно расшифровать и подкаталоги: в ответ на запрос выберите Apply Changes To This Folder, Subfolders, And Files и щелкните OK.

Совет Windows 2000 также предоставляет программу командной строки для шифрования и расшифровки информации — Cipher (CIPHER.EXE). Набрав в командной строке CIPHER, вы узнаете состояние шифровки всех папок текущего каталога.

Глава 11

Администрирование наборов томов и RAID-массивов

При работе с серверами Microsoft Windows 2000 вам придется довольно часто выполнять дополнительную настройку, дисков, например, создавать наборы томов или настраивать RAID-массивы. Бот некоторые задачи, которые можно выполнить из консоли Disk Management (Управление дисками).

- *Создание набора томов.* Вы можете создать том. объединяющий несколько накопителей. Пользователи смогут обращаться к нему, как к обычному диску, не обращая внимания на то, сколько на самом деле накопителей включено в том. Том, включающий один диск, называют *простым,* а несколько — *составным.*
- *Настройка RAID-массивов.* Избыточные массивы независимых дисков (redundant array of independent disks, RAID) позволяют защитить данные, а порой и увеличить производительность дисковой подсистемы. Windows 2000 поддерживает три уровня RAID: 0, 1 и 5. Вы можете настроить RAID-массивы для работы с зеркальными, чередующимися и чередующимися с контролем четности дисками.

Тома в Windows 2000 основаны на динамических дисках. Если вы создали том под Windows NT 4.0, вы должны преобразовать базовые диски с томами в динамические, чтобы управлять старым томом, как любым другим в Windows 2000, иначе возможности управления томами будут ограничены.

Наборы томов и RAID-массивы можно создать только на динамических дисках, я доступны они только в Windows 2000 или более поздней версии. А значит, если на вашем компьютер с двухвариантной загрузкой загружена предыдущая версия Windows, динамические диски будут недоступны.

Впрочем, компьютеры со старыми версиями Windows могут обращаться к таким лискам по сети, как к обычным сетевым дискам.

Использование томов и наборов томов

Создание и управление томами во многом схожи с созданием и управлением разделами. Том — это часть диска, где можно напрямую сохранять данные.

Примечание Если на базовых дисках находятся составные или чередующиеся тома, вы можете удалить том, но не создать или расширить его. Если на базовых дисках находятся зеркальные тома, вы можете удалять, восстанавливать и синхронизировать зеркала. Зеркало можно и отключить. Если на базовых дисках находятся чередующиеся тома с контролем четности (RAID 5), вы можете удалить или восстановить том, но не создать новый.

Основные понятия о томах

Оснастка Disk Management выделяет тома цветом, подобно разделам, в зависимости от тина (рис. 11-1). Тома имеют особенности:

- организация дисков подразумевает простые, составные, зеркальные, чередующиеся и чередующиеся с четностью диски;
- тома всегда основаны на динамических дисках;
- как и разделы, каждый том может иметь свою файловую систему: FAT, FAT 32 или NTFS;
- для каждого диска отображается текущее состояние (см. главу 10) и емкость.

Важное преимущество динамических томов перед базовыми — возможность вносить изменения в тома и диски без последующей перезагрузки системы (в большинстве случаев). Кроме того, тома позволяют задействовать средства отказоустойчивости Windows 2000. Хотя динамические диски с предыдущими версиями Windows использовать нельзя, вы вправе установить другую ОС параллельно с Windows 2000. В случае динамических дисков необходимо создать отдельный том для другой ОС. Например, вы можете установить Windows 2000 на том C, а Linux — на том D.

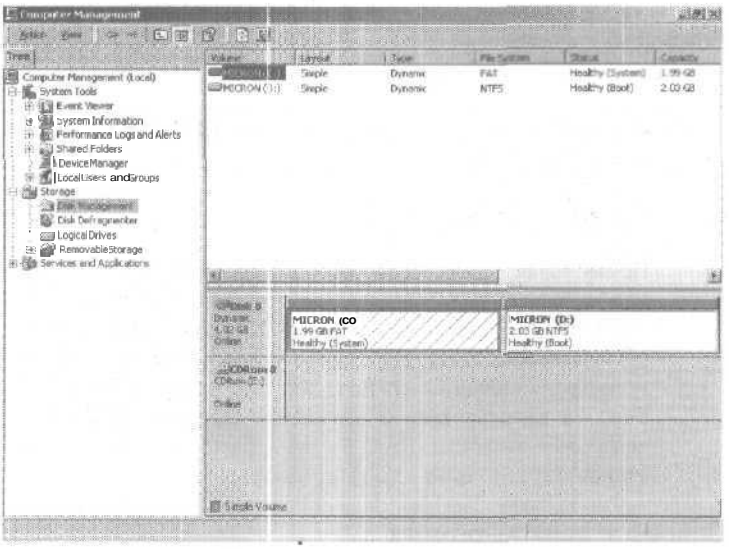


Рис. 11-1. Disk Management показывает тома как разделы.

С томами вы можете:

- определять буквы диска (см. главу 10);
- определять пути (см. главу 10);
- создавать любое количество томов на диске, пока на нем есть свободное место;
- создавать тома, состоящие из двух или более дисков, и включать механизмы отказоустойчивости;
- расширять тома для увеличения емкости тома;
- назначать активный, системный и загрузочный тома (см. главу 10).

Понятие наборов томов

Наборы позволяют создать тома, содержащие несколько дисков. Таким образом, вы используете свободное пространство разных накопителей для создания тома, который будет представляться пользователю как один том. Файлы записываются в набор томов последовательно сегмент за сегментом. Первый сегмент свободного пространства используется первым для записи файла. Когда данный сегмент заполнится, включается второй и т. д.

Вы можете создать набор, используя свободное пространство до 32 дисковых накопителей. Наборы томов позволяют эффективно задействовать свободное пространство и формируют удобную файловую систему. Но если один из накопителей в наборе откажет, выйдет из строя весь набор томов, т. е. все данные в наборе будут утеряны.

Создание томов и наборов томов

Том и набор томов создаются так.

1. В графическом представлении оснастки Disk Management (Управление дисками) щелкните правой кнопкой в области Unallocated (Незанятое место) динамического диска, затем выберите Create Volume (Создать том). Запустится Create Volume Wizard (Мастер создания тома). Прочитайте приглашение и щелкните Next (Далее).
2. Выберите Simple Volume (Простой том), чтобы создать том па одном диске, или Spanned Volume (Составной том) — для создания тома на нескольких (рис. 11-2). Простые тома можно отформатировать под FAT, FAT32 или NTFS. Для упрощения управления дисками отформатируйте тома, объединяющие несколько дисков, под NTFS, так как NTFS позволяет расширять набор томов.

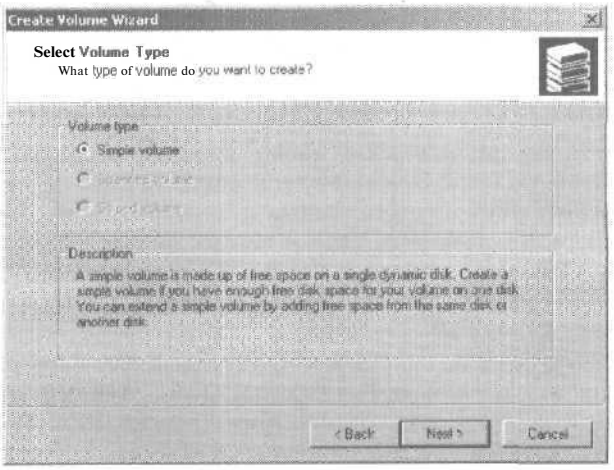


Рис. 11-2. Выберите тип тома и щелкните Next.

Примечание Если вам требуется дополнительное пространство на томе, можно расширить простые и составные

тома, выбрав область свободного пространства и добавив ее к тому. Вы можете расширить том как в пределах одного диска, так и на пространстве другого диска. В последнем случае создается составной том, диски которого должны иметь формат NTFS.

3. В диалоговом окне Select Disks (Выбор дисков) можно выбрать динамический диск для включения в том и задать на нем размер сегмента тома (рис. 11-3).

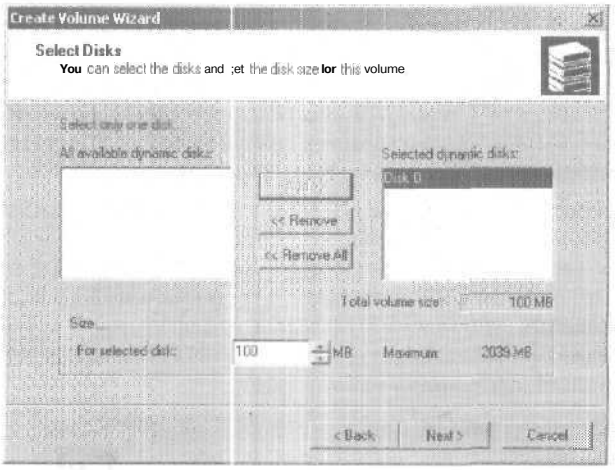


Рис. 11-3. Окно Select Disks позволяет выбрать диски в составе тома и задать размеры тома на каждом диске.

4. Доступные динамические диски показаны в списке AH Available Dynamic Disks (Доступныдинамическиедиски). Выберите диск из этого списка и щелкните Add (Добавить), чтобы добавить диск в список Selected Dynamic Disks (Выбраны динамическиедиски). Если вы ошиблись, можете удалить диск из списка, выбрав его и щелкнув Remove (Удалить).

5. Выберите диск из списка Selected Dynamic Disks и в комбинированном списке For Selected Disk ... MB (На выбранном диске) задайте размер тома на диске. Поле Maximum показывает размер наибольшей области свободного пространства, доступной на выбранном диске. Поле Total Volume Size (Общий размер тома) показывает размер общего дискового пространства, выбранного для тома.

Совет Поскольку размер набора томов можно менять, у вас может возникнуть вопрос: как использовать наборы томов на текущей рабочей станции или сервере? Простые и составные тома не являются отказоустойчивыми. Лучше создать несколько небольших томов, чем один огромный, используя все доступное пространство.

6. Определите, будете ли вы назначать накопителю букву или путь. Вы можете:
   - Assign **Drive** Letter **Or Path** (Назначение буквы диска или пути) — назначить букву диска, выбрав эту команду, а затем — свободную букву в представленном списке;
   - **Mount This Volume At An Empty Folder That Supports Drive Paths** (Подключить том как пустую папку, поддерживающую путь) — назначить путь диска, выбрав эту команду, а затем набрав путь к существующей папке или щелкнув Browse (Обзор), чтобы найти или создать папку;
   - Do Not Assign **A Drive Letter Or Drive Path** (Неназначать букву диска или путь) — назначить букву или путь позже.

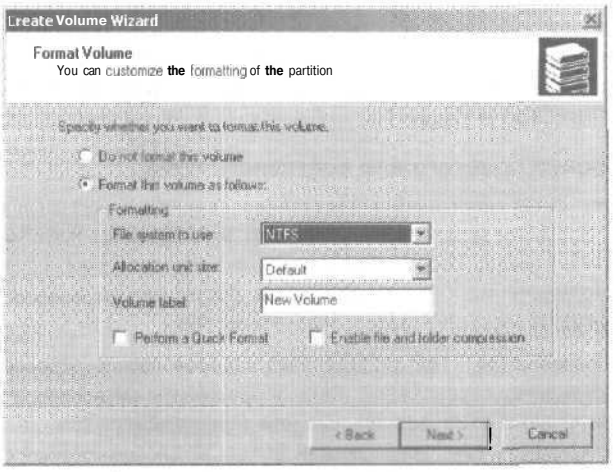


Рис. 11-4. Форматирование тома под определенную файловую систему.

7. Определите, будете ли вы форматировать том (рис. 11-4). Если да, следуйте указаниям по форматированию разделов из главы 10.
8. Щелкните Next, а затем Finish (Готово). Если вы добавили тома на физический диск, содержащий Windows 2000, вы можете по неосторожности изменить номер загрузочного тома. Прочитав предупреждающие сообщения, измените файл BOOT.INI, как описано в главе 10.

Удаление томов и наборов томов

Одним и тем же способом вы можете удалить любые тома: простые, составные, зеркальные, чередующиеся или чередующиеся с контролем четности. Удаление набора томов уничтожит файловую систему и данные. Поэтому, прежде чем это сделать, сохраните копии файлов и каталогов, хранящиеся на наборе.

Тома удаляют так.

1. В оснастке Disk Management правой кнопкой щелкните любой том в наборе и выберите Delete Volume (Удалить том). Вы не сможете удалить часть составного тома, не удалив весь том.
2. Подтвердите желание удалить том, щелкнув Yes (Да).
3. Если вы удаляете том физического диска, содержащего Windows 2000, номер загрузочного раздела может измениться. Если это произошло, измените файл BOOT.INI, как описано в главе 10.

Расширение простого или составного тома

Windows 2000 предлагает несколько способов расширения томов NTFS, не являющихся частью зеркального или чередующегося набора. Вы можете расширить простой том, а также существующие наборы томов. При расширении томов вы добавляете к ним свободное пространство.

Примечание При расширении наборов томов существует множество ограничений. Нельзя расширить загрузочные или системные тома, зеркальные или чередующиеся тома, а также создать том, занимающий более 32 дисков. Нельзя расширить тома FAT или FAT32: сначала нужно преобразовать их в NTFS. Нельзя расширить простые или составные тома, преобразованные из базовых дисков.

Чтобы расширить том NTFS, сделайте так.

1. В оснастке Disk Management правой кнопкой щелкните простой или составной том, который хотите расширить, и выберите Extend Volume (Расширить том). Запустится Extend Volume Wizard (Мастер расширения тома). Прочитайте приглашение и щелкните Next.
2. Теперь вы можете выбрать динамические диски, которые войдут в том, и задать размеры сегментов тома на этих дисках, как описано в пп. 5-7 раздела «Создание томов и наборов томов».

Примечание Набор томов на нескольких накопителях не может быть зеркальным или чередующимся — ими могут быть только простые тома.

3. Щелкните Next, а затем Finish.

Управление томами

Вы можете управлять томами так же, как разделами:

- назначать букву диска и путь;
- изменять и удалять метки тома;
- преобразовывать том в формат NTFS;
- проверять накопитель на ошибки и сбойные секторы;
- дефрагментировать диски;
- сжимать диски и данные;
- шифровать диски и данные.

Подробнее о выполнении этих процедур см. главу 10.

Повышенная производительность и отказоустойчивость RAID-массивов

Важные данные требуют повышенной защиты от сбоев дисков. Для этого вы можете использовать технологию RAID. RAID 1 повышает целостность и доступность данных за счет поддержки копий данных. RAID 5 повышает целостность данных путем создания тома с записью данных и контрольных сумм поочередно на три или более физических дисков. RAID также позволяет увеличить производительность дисков, хотя в RAID 0 при этом не гарантируется целостность данных.

Доступны разные реализации технологии RAID, описываемые уровнями. В настоящее время наиболее распростране-

ны уровни О, 1, 2, 3, 4, 5, 6, 7, 10 и 53. Каждый обладает своими особенностями. Windows 2000 поддерживает уровни О, 1 и 5.

- RAID 0 позволяет увеличить производительность дисков, а также получить дополнительное пространство за счет объединения свободных участков двух или более физических дисков.
- Используйте RAID 1 и 5 для отказоустойчивости.

Ниже дан краткий обзор поддерживаемых уровней RAID (табл. 11-1). Эта полностью программная поддержка доступна только на серверах Windows 2000.

Табл. 11-1. Поддержка RAID под управлением Windows 2000 Server.

Уровень RAID	Тип RAID	Описание	Основные преимущества
0	Чередование дисков	Два или более томов, каждый па отдельном накопителе, сконфигурированы как чередующийся набор. Данные разбиваются на блоки, называемые полосами, и последовательно записываются на все диски в наборе.	Скорость и производительность.
1	Зеркальное отображение дисков	Два тома на двух лисках идентичны. Данные записываются на оба диска. Если один из накопителей отказывает, данные не теряются, так как второй диск содержит их копию.	Избыточность. Выше скорость записи, чем у чередующегося набора с контролем четности.
5	Чередование дисков с контролем четности	Использует три или более томов, каждый на отдельном накопителе, для создания чередующегося набора с контролем ошибок по четности. При сбое данные могут быть восстановлены.	Отказоустойчивость с меньшими затратами, чем при зеркальном отображении. Быстрое чтение по сравнению с зеркальным отображением.

На серверах Windows 2000 чаще применяют RAID 1 (зеркальное отображение дисков) и 5 (чередование с контролем четности). Первый способ защиты данных довольно дорог: здесь используется два одинаковых по размеру тома на двух накопителях для создания избыточного набора данных. Если один из дисков откажет, вы сможете считать данные с другого.

Второй способ требует минимум три диска, но обеспечивает отказоустойчивость с меньшими затратами на единицу емкости, чем первый. Если любой из накопителей откажет, данные будут автоматически восстановлены путем комбинирования блоков данных рабочих дисков с записями четности. Четность (или контрольная сумма) — метод коррекции ошибок, создающий по специальному алгоритму значения, позволяющие восстановить потерянные данные.

Развертывание RAID на серверах Windows 2000

Для серверных систем Windows 2000 поддерживает зеркальное отображение дисков, чередование дисков и чередование дисков с контролем четности.

Примечание Некоторые ОС, например MS-DOS, не поддерживают RAID. Если на вашем компьютере установлены две ОС и одна из них не поддерживает RAID, RAID-диски будут для нее недоступны.

Развертывание RAID 0

RAID уровня 0 подразумевает чередование дисков. Два или более тома, каждый па отдельном накопителе, сконфигурированы как чередующийся набор. Данные, записываемые в набор, разбиваются на блоки — *полосы* (stripes). Полосы записываются последовательно на все диски чередующегося набора. Вы можете развернуть том чередующегося набора максимум на 32 дисках, но, как правило, наборы с 2-5 томами работают быстрее обычных томов. Свыше этих пределов производительность резко падает,

Главное достоинство чередования дисков — скорость. Доступ к данным на нескольких дисках обеспечивается несколькими головками, что заметно повышает производительность. Но за это приходится платить надежностью. Как и в случае с наборами томов, если один из дисков чередующегося набо-

ра выйдет из строя, весь набор уже нельзя будет использовать: все данные будут утеряны. Вам придется повторно создать чередующийся набор и восстановить данные из архивов. Об архивировании и восстановлении данных см. главу 14.

Примечание Загрузочные и системные тома не могут быть частью чередующегося набора. Не используйте чередование дисков на этих томах.

При создании чередующихся томов надо использовать тома приблизительно одинакового размера. Disk Management при вычислении общего объема набора основывается на размере наименьшего тома. В частности, максимальный размер набора кратен размеру наименьшего тома. Так, если у вас три физических диска и размер наименьшего тома — 50 Мб, то максимальный размер чередующегося набора будет 150 Мб.

Увеличить производительность чередующегося набора можно так:

- использовать диски, управляемые отдельными контроллерами, что позволит системе параллельно обращаться к нескольким дискам;
- не использовать диски, содержащие чередующийся набор, для других задач, что позволит дискам сосредоточиться на обслуживании набора.

Чередующийся набор создается так.

1. В графической панели оснастки Disk Management щелкните правой кнопкой область динамического диска, помеченную Unallocated, и выберите Create Volume. Запустится мастер создания тома. Прочитайте приглашение и щелкните Next.
2. Выберите Striped Volume (Чередующийся том) и создайте том, как было описано выше. Однако вам понадобится минимум два динамических диска.
3. Чередующийся том можно использовать, как любой другой том. Вы не сможете расширить уже созданный чередующийся набор, поэтому аккуратно спланируйте набор перед его развертыванием.

Развертывание RAID 1

RAID уровня 1 подразумевает зеркальное отображение дисков. При этом используется два одинаковых по размеру тома на двух накопителях для создания избыточного набора данных. На накопители записываются одинаковые наборы данных, и если один из дисков откажет, данные можно считать с другого.

Зеркальное отображение дисков обеспечивает приблизительно такую же отказоустойчивость, что и чередование дисков с четностью. Но поскольку в зеркальных наборах не генерируются контрольные суммы, как правило, они быстрее ведут запись. С другой стороны, чередующиеся диски с четностью обеспечивают большую производительность чтения, так как операция чтения выполняется с нескольких дисков одновременно.

Основной недостаток зеркального набора — двойное сокращение емкости. Так, зеркало для накопителя емкостью 5 Гб требует другого накопителя того же объема. А значит, для хранения 5 Гб информации потребуется 10 Гб.

Примечание В отличие от чередования дисков при зеркальном отображении дисков вы можете «отразить» любой том, а значит, в случае нужды создать зеркало для загрузочных или системных томов.

Как и при чередовании, желательно, чтобы зеркальные диски обслуживались разными дисковыми контроллерами. Это обеспечит повышенную защиту от сбоев дисковых контроллеров. Если один из контроллеров откажет, диск на другом контроллере будет доступен. Фактически, используя два дисковых контроллера для дублирования данных, вы приходите к технологии *дублированиядисков* (disk duplexing). При зеркальном отображении дисков обычно используют один дисковый контроллер, а при дублировании — два (рис. 11-5).

Если один из зеркальных дисков откажет, дисковые операции могут продолжаться. При записи и чтении данные записываются на оставшийся в работе диск. Перед восстановлением зеркала его нужно отключить (см. раздел «Управление RAID и восстановление после сбоев»).

Создание зеркального набора с помощью Disk Management

1. Б графической панели оснастки Disk Management щелкните правой кнопкой область динамического диска, помеченную Unallocated, а затем выберите Create Volume (Создать том). Запустится мастер создания тома. Прочитайте приглашение и щелкните Next.
2. Выберите Mirrored Volume (Зеркальный том) и создайте том, как описано в разделе «Создание томов и наборов томов». Основное отличие в том, что вам нужно создать два одинаковых по размеру тома на разных динамических дисках.

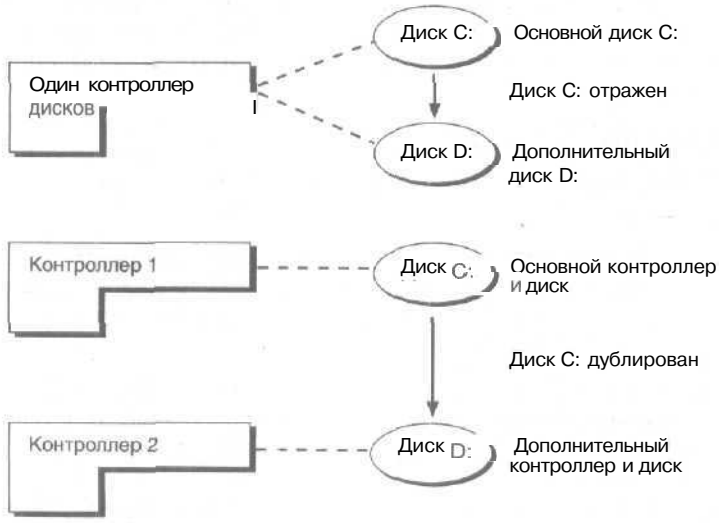


Рис. 11-5. При зеркальном отображении дисков используется один контроллер, а при дублировании — два. Но по существу это одна и та же технология.

3. Как и другие RAID-технологии, зеркальное отображение прозрачно для пользователей, Пользователи видят зеркальный набор как обычный диск и могут обращаться к нему, как к любому другому диску.

Примечание Состояние нормального зеркала — Healthy (Исправен). В процессе создания зеркала вы можете увидеть состояние Initializing (Инициализация), когда оснастка Disk Management сообщает о процессе настройки зеркала.

Зеркальное отображение существующих томов

Для создания зеркального набора можно задействовать существующий простой том. Для этого на втором динамическом диске должно быть столько же или больше неразмеченного пространства, сколько на имеющемся томе.

Для зеркального отображения существующего тома в оснастке Disk Management сделайте так.

1. Правой кнопкой щелкните простой том, для которого хотите создать зеркальное отображение, и щелкните Add Mirror (Добавить зеркало). Запустится мастер добавления зеркала.
2. В диалоговых окнах мастера выберите и параметры второго тома зеркального набора. Выполняемые действия схожи с описанными в разделе «Создание томов и наборов томов».

Развертывание RAID 5

RAID уровня 5 подразумевает чередование дисков с контролем четности. Для реализации этой технологии нужно минимум три жестких диска. Оснастка Disk Management сделает размеры томов на этих дисках одинаковыми. Хотя вы можете разместить тома чередующегося набора максимум на 32 дисках, для достижения наилучшей производительности рекомендуется включать в набор не более 2-5 дисков. Свыше этих пределов скорость резко падает.

По сути RAID 5 — расширенная и отказоустойчивая версия RAID 1. Отказоустойчивость гарантирует, что сбой одного диска не повлияет на работу всего набора. Набор будет функционировать, направляя дисковые операции на оставшиеся и работе тома.

Для обеспечения отказоустойчивости RAID 5 записывает контрольную сумму вместе с блоками данных. Если один из дисков набора выйдет из строя, вы сможете использовать информацию четности для восстановления данных. (Об этом процессе, называемом регенерацией чередующегося набора, см. раздел «Управление RAID и восстановление после сбоев».) С другой стороны, при отказе двух дисков информации четности недостаточно для восстановления данных, и вам придется восстанавливать набор из архива.

Примечание Загрузочные и системные диски не могут быть частью чередующегося тома. Не применяйте чередование для этих дисков.

Создание чередующегося набора с контролем четности с помощью Disk Management

1. В графической панели оснастки Disk Management щелкните правой кнопкой область динамического диска, помеченную Unallocated, и выберите Create Volume (Создать том). Запустится мастер создания тома. Прочитайте приглашение и щелкните Next.
2. Выберите RAID-5 Volume (Том RAID-5) и создайте том, как описано в разделе «Создание томов и наборов томов». Основное отличие *в* том, что вам нужно выбрать свободное пространство на трех отдельных динамических дисках.
3. К созданному чередующемуся набору пользователи могут обращаться, как к обычному диску. Но помните; вы не сможете расширить уже созданный чередующийся набор, добавив дополнительные диски или заменив диски на более емкие. Поэтому особенно аккуратно спланируйте набор перед его развертыванием.

Управление RAID и восстановление после сбоев

Управление зеркальными и чередующимися наборами отличается от управления другими дисковыми томами, особенно при восстановлении после сбоя.

Разрушение зеркального набора

Вам может понадобиться отключить зеркало по двум причинам.

- При отказе одного из дисков зеркального набора операции записи и чтения данных производятся с оставшегося диска. Перед восстановлением зеркала надо разрушить набор.
- Если зеркальное отображение дисков больше не требуется, зеркало можно разрушить. Это позволит использовать освободившееся место на зеркальном диске в других целях.

Примечание Хотя разрушение зеркала не влечет удаления данных, следузт всегда делать архивные копии перед

выполнением этой процедуры. Тогда при возникновении проблем вы сможете восстановить данные.

Зеркало можно разрушить в Disk Management.

1. Щелкнув один из томов зеркального набора правой кнопкой, выберите Break Mirror.
2. Подтвердите желание разрушить зеркало, щелкнув Yes. Будет создано два независимых тома.

Ресинхронизация и восстановление зеркального набора

Windows 2000 автоматически синхронизирует зеркальные тома на динамических дисках, но данные на зеркальных дисках могут рассинхронизироваться. Так, если один диск отключается, данные записываются только на подключенный диск.

Вы можете ресинхронизировать или восстановить зеркальные наборы на базовых и динамических дисках, но для этого нужно перестроить набор на базе диска того же типа, Для ресинхронизации отказавшего дискового набора сделайте так.

1. Оба диска зеркального набора должны быть подключены и доступны. Статус зеркального набора должен быть Failed Redundancy. Предпринимаемые вами действия зависят от статуса отказавшего тома.
2. Если статус — Missing (Отсутствует) или Offline (Не подключен), убедитесь, что на диск подается электропитание и он правильно подключен. Затем запустите Disk Management, правой кнопкой щелкните отказавший том и выберите Reactivate Disk. Статус диска должен измениться на Regenerating (Регенерация), а затем на Healthy (Исправен). Если статус не поменялся на Healthy, щелкните том правой кнопкой и выберите Resynchronize Mirror.
3. Если статус — Online (Errors), щелкните правой кнопкой отказавший том и выберите Reactivate Disk. Статус диска должен измениться на Regenerating, а затем на Healthy. Если статус не поменялся на Healthy, правой кнопкой щелкните том и выберите Resynchronize Mirror (Синхронизировать зеркало).
4. Если один или несколько дисков помечены Unreadable, вам, возможно, надо повторить сканирование дисков в системе, выбрав команду Rescan Disks из меню Action (Действие). Если статус дисков не изменился, перезагрузите компьютер.

5. Если один из дисков так и не вернулся в подключенное состояние, щелкните правой кнопкой отказавший том и выберите Remove Mirror (Удалить зеркало). Затем правой кнопкой щелкните оставшийся том зеркала и выберите Add Mirror (Добавить зеркало). Вам понадобится неразмеченная область для зеркального отображения тома. Если на диске нет свободного места, удалите другие тома или заменить отказавший диск.

Восстановление зеркального системного диска с возможностью загрузки

Сбой зеркального диска может помешать загрузке системы. Обычно это происходит, когда в процессе зеркального отображения системного или загрузочного диска отказывает основной зеркальный диск. Вы решите проблему, заменив отказавший накопитель и настроив систему для загрузки с другого накопителя с помощью аварийного загрузочного диска (о его создании см. главу 14).

Редактирование BOOT.INI для зеркала

Поскольку у вас есть аварийный загрузочный диск, отредактируйте файл BOOT.INI, чтобы ОС могла загрузиться со второго диска. Этот файл содержит примерно такие записи:

```
[boot loader] timeout=30
default=multi(0)disk(0)rdisk(0)volume(2)\WIN2000[operating
systems]multi(0)disk(0)rdisk(0)volume(2)\WIN2000="Windows
2000Server"
```

Если зеркальный диск — на накопителе 2, измените файл BOOT.INI:

```
[boot loader] timeout=30
default=multi(0)disk(0)rdisk(1)volume(2)\WIN2000[operating
systems]multi(0)disk(0)rdisk(1)volume(2)\WIN2000=""Windows
2000Server"
```

Примечание Подробнее о файле BOOT.INI см. главу 10.

Загрузка и перезагрузка системы

Если вы модифицировали файл BOOT.INI, вы можете загрузить систему с аварийного загрузочного диска. Когда загрузка завершится, сделайте так.

1. Отключите зеркальный набор, а затем воссоздайте зеркало на замененном диске, который станет накопителем 0. Правой кнопкой щелкните оставшийся том из оригинального зеркального набора и выберите Add Mirror. Далее следуйте указаниям из раздела «Зеркальное отображение существующего тома*.
2. По завершении создания зеркального отображения повторно разрушьте зеркало из оснастки Disk Management. Убедитесь, что основной диск в оригинальном зеркальном наборе получил букву, которая ранее была у набора. Если это не так, назначьте соответствующую букву.
3. Правой кнопкой щелкните **оригинальный** системный том и выберите Add Mirror. Зеркало будет **воссоздано.**
4. Измените файл BOOT.INI, чтобы система загружалась с исходного системного диска.

Удаление зеркального тома

Из оснастки Disk Management можно удалить один из томов зеркального набора. Когда вы это сделаете, все данные с удаленного тома будут стерты, а освободившееся пространство помечено Unallocated.

Зеркальный том удаляется так.

1. В оснастке Disk Management щелкните правой кнопкой один из томов зеркального набора и выберите Remove Mirror.
2. Подтвердите свои действия. Все данные на удаленном томе будут уничтожены,

Восстановление чередующегося набора без записи контрольных сумм

Такой чередующийся набор не обеспечивает отказоустойчивости. Если один из дисков в наборе откажет, весь набор становится непригодным. Перед попыткой восстановить набор надо восстановить или заменить отказавший накопитель, воссоздать набор, а затем восстановить данные из архива,

Регенерация чередующегося набора с контролем четности

RATD 5 позволяет восстановить чередующийся набор при отказе одного диска. Как вы знаете, при отказе диска статус

набора изменяется на Failed Redundancy, а статус отдельного тома — на Missing, Offline или Online (Errors).

Вы можете восстановить RAID 5 на базовых или динамических дисках, но вам нужно перестроить набор, используя тот же тип дисков.

1. Все диски набора НАШ 5 должны быть подключены. Статус набора должен быть Failed Redundancy. Ваши действия зависят от статуса отказавшего тома.

Примечание По возможности сделайте архивные копии данных перед выполнением этой процедуры. Тогда при возникновении проблем вы сможете восстановить данные.

2. Если статус — Missing или Offline, убедитесь, что на диск подается электропитание и он правильно подключен. Затем запустите Disk Management, правой кнопкой щелкните отказавший том и выберите Reactivate Disk. Статус диска должен измениться на Regenerating (Восстановление), а затем на Healthy. Если статус не поменялся на Healthy, правой кнопкой щелкните том и выберите Regenerate Parity (Восстановить четность).
3. Если статус — Online (Errors), правой кнопкой щелкните отказавший том я выберите Reactivate Disk. Статус диска должен измениться на Regenerating, а затем на Healthy. Если статус не поменялся на Healthy, щелкните правой кнопкой том и выберите Regenerate Parity.
4. Если один или несколько дисков помечены Unreadable, возможно, следует пересканировать диски в системе, выбрав команду Rescan Disks в меню Action. Если статус дисков не изменился, перезагрузите компьютер.
5. Если один из дисков так и не вернулся к подключенному состоянию, восстановите сбойную область набора RAID 5. Правой кнопкой щелкните отказавший том и выберите Remove Volume (Удалить том). Затем выберите неразмеченную область на отдельном динамическом диске набора. Она должна быть не меньше восстанавливаемой области. Свободное место должно располагаться на диске, не используемом в текущий момент набором RAID 5. Если свободного места не хватает, команда Repair Volume (Восстановить том) будет недоступна: освободите дисковое пространство, удалив другие тома или заменив отказавший накопитель.

Глава 12

Управление файлами и каталогами

Microsoft Windows 2000 предоставляет мощные средства для работы с файлами и каталогами. В основе этих средств - два базовых типа файловых систем:

- таблица размещения файлов (file allocation table, FAT) существует в 16-битной и 32-битной версиях;
- файловая система Windows NT (Windows NT file system, NTFS) доступна в версиях 4.0 и 5.0.

Файловые структуры Windows 2000

Понимание основ организации файлов значительно облегчает работу администратора.

Основные свойства FAT и NTFS

Возможности работы с файлами и каталогами в Windows 2000 зависят от тина файловой системы. Серверы и рабочие станции Windows 2000 поддерживают FAT и NTFS.

Тома FAT

Тома FAT отслеживают состояние файлов и каталогов по таблице размещения. Однако возможности FAT ограниченны. Windows 2000 поддерживает две версии FAT (табл. 12-1).

- FAT16 широко используется в Microsoft Windows NT 4.0. FAT16 поддерживает 16-битную таблицу размещения файлов, и обычно ее называют просто FAT Эта система оптимальна для томов размером менее 2 Гб.
- FAT32 появилась во втором выпуске Windows 95 (OSR 2) и поставлялась с Windows 98. FAT32 поддерживает 32-битную таблицу размещения файлов кластеры меньшего размера, чем FAT, за счет чего эффективнее использует

пространство диска. В Windows 2000 FAT32 поддерживает тома размером "до 32 Гб.

Табл. 12-1. Сравнение характеристик FAT и FAT32.

Характеристика	FAT	FAT32
Размер элемента таблицы размещения файлов	16 бит	32 бита
Максимальный размер раздела	4 Гб; наилучший — до 2 Гб	2 Тб; ограничен в Windows 2000 до 32 Гб
Максимальный размер файла	2 Гб	4 Гб
Поддерживается операционными системами	MS-DOS, все версии Windows	Windows 95 OSR 2, Windows 98 и Windows 2000
Поддерживает малый размер кластеров	Нет	Да
Поддерживает возможности NTFS 4,0	Нет	Нет
Поддерживает возможности NTFS 5,0	Нет	Нет
Используется на дискетах	Да	Да
Используется на съемных носителях	Да	Да

Использование NTFS

NTFS предлагает мощные средства для работы с файлами и каталогами. Существу от две версии NTFS.

- NTFS 4.0 используется в Windows NT 4.0. Полностью поддерживает управление локальным и удаленным доступом к файлам и каталогам, а также технологии сжатия файлов и каталогов Windows. Не поддерживает большую часть возможностей файловой системы Windows 2000.
- NTFS 5.0 используется в Windows 2000. Полностью поддерживает такие возможности Windows 2000, как служба каталогов Active Directory, дисковые квоты и шифрование. Эта система поддерживается только в Windows 2000 и минимально — в Windows NT 4.0 SP4 или более поздними выпусками.

Примечание Если вы создали разделы NTFS в Windows NT 4.0 и обновили систему до Windows 2000, разделы не

обновляются автоматически до NTFS 5.0. Вы должны явно выбрать обновление разделов при установке ОС или при установке Active Directory на сервер Windows 2000.

Ниже дано краткое сравнение характеристик NTFS 4.0 и NTFS 5.0 (табл. 12-2). Системы Windows NT 4.0 SP4 или более поздние могут обращаться к файлам и каталогам NTFS 5.0, но не используют все новые возможности NTFS.

Табл. 12-2. Сравнение характеристик NTFS 4.0 и NTFS 5.O.

Характеристика	NTFS 4.0	NTFS 5.0
Максимальный размер раздела	32 Гб	2 То
Максимальный размер файла	32 Гб	Ограничен только размером раздела
Поддерживается операционными системами	Windows NT 4.0, Windows 2000	Windows 2000 и Windows NT 4.0 не полностью
Расширенные права доступа к файлам	Да	Да
Поддерживает сжатие Windows	Да	Да
Поддерживает шифрование Windows	Нет	Да
Поддерживает структуры Active Directory	Нет	Да
Поддерживает разреженные файлы	Нет	Да
Поддерживает внешнее хранилище	Нет	Да
Поддерживает дисковые квоты	Нет	Да
Используется на дискетах	Нет	Нет
Используется на съемных носителях	Да	Да

Имена файлов

Соглашения Windows 2000 об именах файлов применяются и к файлам, и к каталогам. Для простоты термин «наименование файла» часто применяют но отношению и к файлам, и к каталогам. Хотя имена файлов Windows 2000 могут содержать и прописные, и строчные буквы, от регистра они не зависят. Это значит, что вы можете сохранить файл MyBook.doc

и имя файла будет показано именно в таком виде. Однако вы не сможете сохранить в том же каталоге файл mybook.doc.

И NTFS, и FAT32 поддерживают длинные имена файлов - до 255 символов. Вы можете называть файлы, используя почти все символы, включай пробелы, кроме:

? * / \ : « o I

Совет Пробелы в именах файлов могут стать причиной проблем с доступом к ним. При ссылке на такой файл может понадобиться взять его имя в кавычки. Кроме того, если вы планируете опубликовать этот файл в Интернете, вам, возможно, придется удалить все пробелы из имени файла или заменить их символами подчеркивания (_), чтобы обозреватели гарантированно получили доступ к вашему файлу.

Допустимы следующие имена файлов:

- My Favorite Short Story.doc;
- My_Favorite_Short_Story.doc;
- My..Favorite..Short. Story.doc;
- My Favorite Short Story!!!.doc.

Доступ к длинным именам файлов из MS-DOS

В MS-DOS с 16-битной файловой системой FAT имена файлов и каталогов ограничены 8 символами и 3 символами расширения файла, например C1IAPTER4.TXT. Это соглашение об именах часто называют правилом 8.3 или стандартным правилом именования файлов MS-DOS. Из-за этого при обращении к файлам и каталогам из утилит командной строки, не поддерживающих длинные имена, могут возникнуть проблемы.

Для поддержки доступа к длинным именам для всех файлов и каталогов в системе создаются сокращенные имена, соответствующие стандартным правилам именования файлов MS-DOS. Увидеть сокращенные имена файлов позволяет команда:

```
dir /X
```

Обычно сокращенное имя файла выглядит примерно так:

```
PROGRA-1.DOC
```

Как Windows **2000 создает сокращенное имя файла**

Windows 2000 создает сокращенное имя файла из длинного по следующим правилам:

- все пробелы в имени файла удаляются: имя файла My Favorite Short Story.doc превращается в MyFavoriteShort-Story.doc;
- все точки в имени файла удаляются (кроме точки, отделяющей имя файла от его расширения): имя файла My..Favorite..Short..Story.doc превращается в MyFavoriteShort-Story.doc;
- недопустимые по правилам именования файлов в MS-DOS символы заменяются символом подчеркивания (_): имя файла My[Favorite]ShortStory.doc превращается в My_Favorite_ShortStory.doc;
- все оставшиеся символы переводятся в верхний регистр: имя файла My Favorite Short Story.doc превращается в MYFAVORITESHORTSTORY.DOC.

Затем применяются правила сокращения для создания стандартного *имени* файла MS-DOS.

Правила сокращения

Для приведения к виду 8.3 имя файла и его расширение сокращаются, если это необходимо.

- Расширение файла сокращается до первых трех символов: имя файла Mary.text становится MARY.TEX.
- Имя файла сокращается до первых 6 символов (это корневое имя файла), и добавляется уникальный указатель вида *~n,* где *n* — номер файла с 6-символьным именем: имя файла My Favorite Short Story.doc превращается в MYFAVO~1.DOC; второй файл в том же каталоге, у которого имя сократится до MYFAVO, станет MYFAVO~2.DOC.

Примечание Если у вас много файлов с похожими именами, вы можете увидеть результат применения другого правила создания короткого имени файла. Если более 4 файлов используют одинаковый 6-символьный корень, дополнительные имена файлов создаются комбинацией первых двух символов имени файла и 4-символьного хэш-кода с добавлением затем уникального указателя. Если в каталоге хранятся файлы MYFAVO~1.DOC, MYFAVO~2.DOC,

MYFAVO~3.DOC и MYFAVO~4.DOC, дополнительные файлы с этим корнем могут быть названы MY3140~1.DOC, MY40C7~1.DOC, и MYEACC~1.DOC.

Просмотр файлов и каталогов

Работу с файлами и каталогами облечает Windows Explorer (Проводник), однако для этого можно также использовать окна My Computer (Мой компьютер) и My Network Places (Мое сетевое окружение) — их открывает двойной щелчок соответствующих значков на рабочем столе Windows 2000.

Примечание Для краткости я буду в основном говорить о Проводнике, но аналогичные действия можно выполнить и в окнах My Computer и My Network Places.

Использование Проводника Windows

Чтобы запустить Проводник, раскройте меню Start\Programs\Accessories (Пуск\Программы\Стандартные) и выберите Windows Explorer (Проводник).

Виды и панели инструментов Проводника

Проводник может отображать несколько панелей просмотра.

- Вид левой панели Проводника зависит от текущего режима просмотра: Folders (Папки), Search (Поиск), History (История) и Favorites (Избранное). По умолчанию отображаются папки.
- В правой панели отображается содержимое выбранной папки или результат поиска.
- В области Tip Of The Day (Полезный совет) выводятся полезные указания по работе с Windows 2000.

Вид отдельных папок также можно настраивать (рис. 12-1). По умолчанию Проводник отображает только панели обозревателя и содержимого, но вы можете потребовать:

- **показать** другие **виды на панели обозревателя:** выберите меню View (Вид), Explorer Bar (Панель обозревателя) и затем — нужный вам вид;
- **показать совет:** выберите меню View (Вид), Explorer Bar (Панель обозревателя) и затем — Tip Of The Day (Полезный совет);

- **убрать панель обозревателя или совет:** щелкните кнопку закрытия панели (значок X в верхнем левом или верхнем правом углу панели).

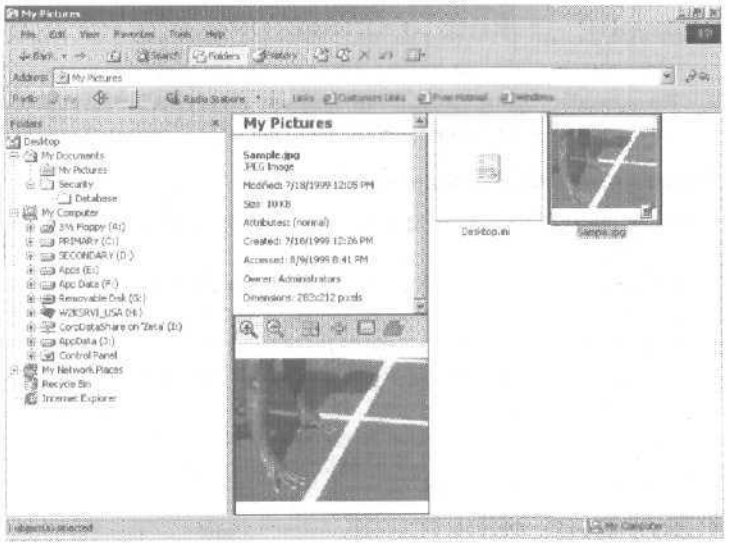


Рис. 12-1. Вид папки My Pictures (Мои рисунки) настроен пользователем. Вы можете настроить для папок Проводника обычный вид или любой другой. Ваши параметры сохранятся и после завершения сеанса.

Изменить вид содержимого позволяет также меню View (Вид). Помеченные галочкой пункты включены, остальные — выключены. Основные параметры таковы:

- **Toolbar** (Панель инструментов) позволяет добавить и убрать панели инструментов;
- **Status Bar** (Строка состояния) добавляет строку состояния, которая отображает информацию о выбранных объектах;
- List (Список) отображает список файлов и папок вместо значков или подробного списка (таблицы);
- **Details** (Таблица) отображает подробный список файлов и папок, для каждого объекта на панели содержимого указывается размер, тип файла и дата изменения;
- Small **Icons** (Мелкие значки) отображает мелкие значки для файлов и папок;

- **Large Icons** (Крупные значки) отображает крупные значки для файлов и папок;
- **Arrange Icons** (Упорядочить значки) позволяет упорядочить файлы и папки по именам, типу, размеру и дате, при отображении в виде таблицы щелчок заголовка соответствующего столбца имеет аналогичный эффект;
- **Thumbnails** (Миниатюры) позволяет видеть миниатюрную версию файла изображения для быстрого просмотра.

Понятие о значках Проводника Windows

Каждый значок, отображаемый в Проводнике, имеет свое назначение.

- **Desktop** (Рабочий стол) — папка верхнего уровня, где хранятся файлы, папки и ярлыки рабочего стола Windows. Она находится на том же уровне иерархии, что и My Network Places (Сетевое окружение) и My Computer (Мой компьютер).
- **My Computer** (Мой компьютер) — папка верхнего уровня, содержащая все локальные ресурсы и папки, доступные данному компьютеру.
- My Network **Places;** (Сетевое окружение) — папка верхнего уровня для сети. Щелкните ее для просмотра сетевых ресурсов.
- **Recycle Bin** (Корзина) — папка, где хранятся удаленные файлы и каталоги. Если система настроена для использования корзины, вы можете восстанавливать файлы из нее до того, как они будут окончательно удалены.
- **My Documents** (Мои документы) — папка для хранения личных файлов. Она хранит папку My Pictures (Мои рисунки), настроенную для предварительного просмотра изображений.
- **Диски** — устройства хранения, каждое из которых идентифицируются уникальным значком и буквой диска. Windows 2000 отображает разделы жестких дисков, гибкие диски, съемные диски и компакт-диски.
- **Сетевые диски** — удаленные сетевые ресурсы, подключенные к системе.
- **Открытые папки** — папки, раскрытые для просмотра; их содержимое показано на правой панели.

- **Закрытые папки** — папки, которые в данный момент не раскрыты для просмотра; их содержимое не показывается.

Совет Чтобы раскрыть папку без показа ее содержимого, в панели содержимого щелкните символ «плюс» (+) слева от названия папки. Таким образом можно просматривать папки на удаленных системах быстрее, чем обычно.
Эта методика удобна и при копировании. При этом вы отображаете содержимое папки, файлы из которой вы хотите копировать, в панели содержимого, затем ищете папку назначения в панели папок и, найдя, копируете в нее исходные файлы.

Отображение скрытых и сжатых файлов в Проводнике Windows

Администратору часто приходится просматривать системные файлы типа динамически подключаемых библиотек (dynamic-link library, DLL), а также сжатые или несжатые файлы. Но по умолчанию Проводник не показывает файлы с атрибутом «скрытый», как не показывает разницу между сжатыми и несжатыми файлами. Чтобы изменить начальные параметры, в меню Tools (Сервис) выберите пункт Folder Options (Свойства папки), а затем вкладку View (Вид). Теперь вы можете настроить новые параметры в диалоговом окне Folder Options (рис. 12-2).

- Чтобы отобразить скрытые файлы, щелкните Show Hidden Files And Folders (Показать скрытые файлы и папки).
- Чтобы отобразить все расширения файлов, снимите флажок Hide File Extensions For Known File Types (Не показывать расширения для известных типов файлов).
- Чтобы отобразить скрытые файлы ОС, снимите флажок Hide Protected Operating System Files (Не показывать защищенные файлы операционной системы).
- Для подсвечивания сжатых файлов и папок пометьте флажок Display Compressed Files And Folders With Alternate Color (Показать сжатые файлы и папки другим цветом).

Настройка вида папки

Проводник позволяет настроить вид папок (как отдельно взятых, так и всех сразу), отображаемых как Web-страницы.

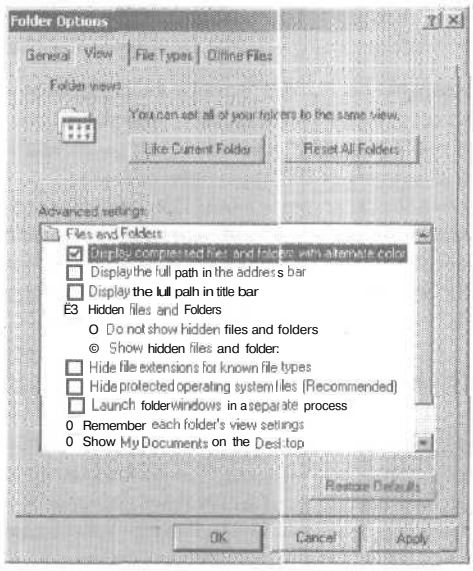


Рис. 12-2. Параметры Проводника настраиваются в диалоговом окне Folder Options.

Работа с шаблонами папок

Используя файлы шаблонов, Проводник определяет, как папка будет выглядеть в панели содержимого. Он создает эти шаблоны как HTML-документы, и вы можете редактировать их как обычный Web-документ. Для создания шаблонов применяются технологии HTML, CSS и сценарии. Сценарии позволяют настроить папки и сделать их более интерактивными. Обычно сценарии пишут на языке JavaScript, но они могут быть написаны и на VBScript. Предопределенные шаблонытаковы:

- **Standard** (Стандартный) обладает всеми возможностями предварительного просмотра документов и аннотаций;
- **Classic (Icons** Only) [Классический (Только значки)] - быстрый и эффективный простой вид;
- **Simple** (Простой) — основной вид, имеющий некоторые возможности Web, но не использующий сценарии;
- **Image Preview** (Просмотр изображений) — вид со специальной возможностью предварительного просмотра изображений.

Параметры пила папки применяются ко всем пользователям, обращающимся к системе как локально, так и удаленно. По умолчанию большинство папок отображаются в стандартном виде. Вы можете изменить вид, настроив папку, если у вас есть нрава записи в нее. Если вам нравится какой-то особый вид, можете применить его ко всем папкам в системе, владельцем которых вы являетесь.

Примечание В стандартном виде окно предварительного просмотра выводит изображения/документы, которые можно показать. Для этого ОС запускает нужное приложение, считывает документ/изображение и показывает его предварительный вид.

Вы также можете добавить для папки фон и комментарий. Фон отображается «позади» всех значков и текста папки. Комментарии показываются на панели аннотации, и в них можно описать содержимое данной папки. Фон и комментарии добавляются в шаблон папки как пользовательские параметры.

Разрешение отображения папок в виде Web-страниц

Шаблоны папок используются, только когда разрешено отображение папок как Web-страниц. Разрешение или запрет этой возможности основаны на наборах параметров Проводника, разных для каждого пользователя, регистрирующегося на компьютере. Отображение папок как Web-страниц разрешается или запрещается так.

1. В Проводнике в меню Tools (Сервис) выберите Folders Options (Свойства папки).
2. На вкладке General (Общие) выберите Enable Web Content In Folders (Отображать веб-содержимое в папках) или Use Windows Classic Folders (Использовать обычные папки Windows).
3. Щелкните OK.

Настройка пользовательского вида папки

1. В Проводнике выберите нужную папку. Чтобы настроить все папки в системе, выберите любую и следуйте инструкциям из раздела «Настройка вида нескольких папок».
2. В меню View (Вид) выберите Customize This Folder (Настроить вид папки). Запустится мастер Customize This

Folder (Настройка папки). Прочитайте информацию во вступительном окне и щелкните Next (Далее).

3. Выберите тип настройки (рис.12-3):
   - **Choose Or Edit An HTML Template For This Folder** (Выбрать или изменить HTML-шаблон для этой папки) позволяет выбрать/создать шаблон для папки;
   - **Modify Background Picture And Filename Appearance** (Изменить рисунок фона и представление имен файлов) позволяет добавить фоновый цвет или рисунок в папку;
   - **Add Folder Comment** (Добавить комментарий к папке) позволяет ввести комментарий-описание папки.

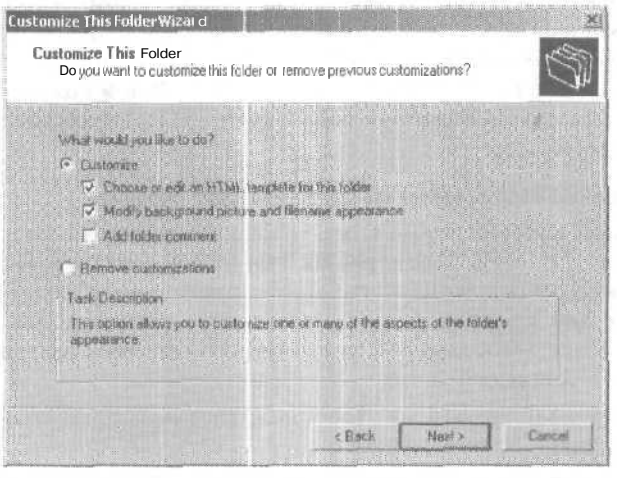


Рис. 12-3. Мастер Customize This Folder (Настройка папки) позволяет выбрать шаблон папки. Шаблон папки создается на базе кода HTML, CSS и сценариев.

4. В окне Change Folder Template (Изменить шаблон папки) можно выбрать новый шаблон. Варианты выбора: Standard (Стандартный), Classic (Icons Only) [Классический (Только значки)], Simple (Простой), Image Preview (Просмотр изображений). Если хотите отредактировать файл шаблона, выберите I Want To Edit This Template (Я хочу изменить этот шаблон).

Внимание! Файлы шаблонов пишут, используя современные технологии создания сценариев. Если у вас есть опыт такой работы, вы легко измените файлы шаблонов. Но будьте осторожны. Неправильное редактирование сделает шаблон неработоспособным, и вам придется назначать папке новый шаблон еще раз.

5. Если вы пометили флажок Modify Background And Filename Appearance (Изменить рисунок фона и представление имен файлов), откроется одноименное окно, где можно выбрать параметры фона и текста. Вы можете выбрать фоновый рисунок из списка или найти изображение, щелкнув кнопку Browse (Обзор). После выбора изображения вы можете, щелкнув кнопку Text (Текст) или Background (Фон), изменить цвета фона и текста (рис.12-4).

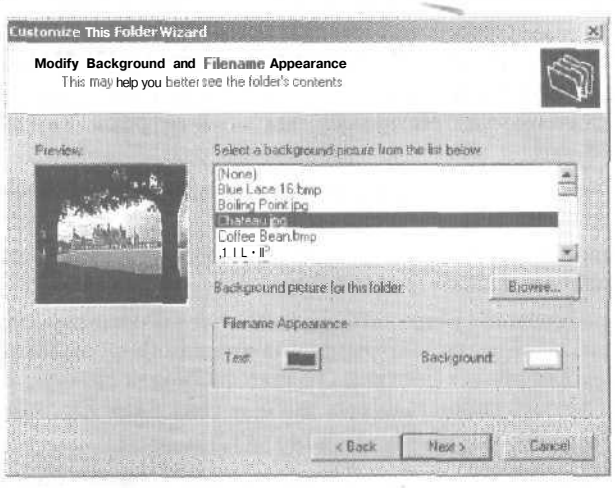


Рис. 12-4. Выберите рисунок фона и измените внешний вид имен файлов.

6. Если вы ранее пометили флажок Add Folder Comment (Добавить комментарий к папке), откроется одноименное окно ввода комментария. Если вы планируете применить этот шаблон ко всем папкам в системе, оставьте пока это поле пустым.

7. **Щелкните** Next, а затем — Finish (Готово). Папка **примет** заданный вид.

Настройка вида нескольких папок

Диалоговое окно Folder Options (Свойства папки) позволяет применить заданный вами вид ко всем папкам в системе или восстановить стандартный вид всех папок.

1. В Проводнике выберите нужную папку. Вы можете применить параметры вида этой папки ко всем вашим папкам в системе,
2. В меню Tools (Средства) выберите Folder Options (Свойства папки) и перейдите на вкладку View (Вид).
3. *Для* применения вида текущей **папки ко** всем вашим папкам **в системе** щелкните Like **Current Folder** (Как у текущей **папки).**
4. Чтобы восстановить стандартный вид всех своих папок, щелкните Reset All Folders (Сброс для всех папок).

Форматирование дискет и других съемных носителей

Проводник упрощает работу с дискетами и другими съемными носителями. Например, вы можете форматировать диски.

1. Вставьте дискету или другой съемный диск, который хотите отформатировать.
2. Правой кнопкой щелкните значок соответствующего диска на панели папок Проводника.
3. В контекстном меню выберите Format (Форматировать), затем задайте параметры форматирования в диалоговом окне. Для дискет доступна только файловая система FAT. Для других типов съемных дисков, таких как Zip, можно использовать FAT, FAT32 или NTFS.

Примечание Если вы форматируете съемный диск как раздел NTFS, на нем создается раздел NTFS 5.O. Windows 2000 в отличие от Windows NT 4.0 позволяет извлечь раздел, отформатированный как NTFS, в любое время. Щелкните кнопку выброса на приводе съемного диска или правой кнопкой щелкните значок диска в Проводнике Windows и выберите Eject (Извлечь).

4. Щелкните Start (Начать) для форматирования дискеты или другого съемного диска.

Копирование дискет

1. Правой кнопкой щелкните значок дискеты на панели папок Проводника и из контекстного меню выберите Copy Disk (Копировать диск).
2. Диалоговое окно Copy Disk (Копировать диск) позволяет выбрать исходный диск и диск назначения. В поле Copy From (Копировать с) укажите диск, который хотите использовать как исходный. В поле Copy To (Копировать на) выберите диск, куда будут скопированы данные. Если у вас на компьютере только один привод для гибких дисков, исходный дисковод и дисковод назначения будут одинаковыми (рис. 12-5).
3. Щелкните Start (Начать), а затем после соответствующих подсказок вставьте исходный диск и диск назначения. Индикатор в нижней части окна копирования диска показывает состояние процесса.

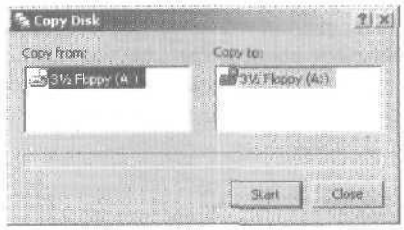


Рис. 12-5. Диалоговое окно Copy Disk позволяет выбрать исходный диск и диск назначения.

Управление файлами

Windows 2000 позволяет управлять файлами многими способами. Вы можете копировать или перемещать файлы *внутри* окон (как в Проводнике) и *между* окнами — например, копируя файл из Проводника Windows в окно My Network Places (Мое сетевое окружение). Вы также можете копировать файлы на рабочий стол и с него.

Выбор файлов и каталогов

Отдельный файл или несколько файлов в Проводнике можно выбрать по-разному. Отдельный файл выбирается щелчком, а несколько файлов:

- при нажатой клавише Ctrl: щелчками нужных файлов:

- при нажатой клавише **Shift:** выбрав первый файл/панку, а затем — последний файл/папку из **нужного** списка.

Копирование файлов и папок перетаскиванием

Вы можете скопировать или переместить объекты в любое открытое окно или видимую область на рабочем столе.

1. Выберите объекты, которые хотите скопировать или переместить.
2. Перетащите мышью эти объекты в новое место.
3. Если вы перетаскиваете файл или папку на другой диск, они автоматически скопируются. Чтобы переместить файл, при перетаскивании удерживайте нажатой клавишу Shift.
4. Если вы перетаскиваете файл/папку в новое место на том же диске, Windows 2000 попытается сразу переместить этот объект. Для предотвращения этого при перетаскивании удерживайте нажатой клавишу Ctrl.

Примечание При копировании исходное местоположение файла и место назначения должны быть видны. Это значит, что вам может понадобиться открыть несколько копий Проводника или несколько окон и раскрыть папки внутри этих окон.

Копирование файлов и папок в места, которые не отображаются в данный момент

Вы можете скопировать объекты в места, не отображаемые в данный момент.

1. Выберите объекты для копирования.
2. Перетащите объекты в панель папок.
3. Медленно подтащите объекты к самой верхней папке, видимой на панели (или к самой нижней). Дерево папок начнет «прокручиваться» вверх или вниз.
4. Дойдя до папки назначения, отпустите кнопку мыши. Если эта папка находится на другом диске, объект скопируется; иначе он будет перемещен.

Копирование и вставка файлов

Я предпочитаю перемещать файлы с помощью операций копирования и вставки. При этом не нужно беспокоиться о том, был файл скопирован или перемещен. Вы просто копируете файлы в буфер обмена и вставляете их, куда нужно.

1. Выберите объекты, которые хотите скопировать,
2. Щелкните их правой кнопкой и выберите Copy (Копировать). Вы можете также выбрать Copy из меню Edit (Правка) или нажать Ctrl+C.
3. Укажите место назначения, щелкните правой кнопкой в любом месте панели содержимого и выберите Paste (Вставить). Вы также можете выбрать Paste из меню Edit (Правка) или нажать Ctrl+V.

Примечание Windows 2000 может не скопировать файлы и папки в специальные окна. Например, обычно нельзя копировать файлы и затем вставить их в окно My Computer (Мой компьютер). Аналогично у вас может не получиться копирование и вставка в другие окна специальных папок.

Перемещение файлов вырезанием и вставкой

1. Выберите объекты, которые хотите переместить.
2. Щелкните их правой кнопкой и выберите Cut (Вырезать). Вы можете также выбрать Cut из меню Edit (Правка) или нажать Ctrl+X.
3. Укажите место назначения, щелкните правой кнопкой в *любом* месте панели содержимого и выберите Paste (Вставить). Вы также можете выбрать Paste из меню Edit (Правка) или нажать Ctrl+V.
4. *Когда появится подсказка переместить* выбранные объекты, щелкните OK.

Примечание Когда вы используете команды Cut и Paste, Windows 2000 не сразу удаляет объект из первоначального местоположения. Команда Cut просто копирует объект в буфер обмена. Файл удаляется со старого места после команды Paste.

Переименование файлов и каталогов

1. Правой кнопкой *щелкните* имя *файла/каталога* и выберите Rename (Переименовать). Или выберите имя файла/каталога, а затем в меню File — Rename.
2. Имя ресурса теперь можно редактировать. Наберите новое имя ресурса.
3. Нажмите Enter или щелкните значок ресурса.

Удаление файлов и каталогов

1. Выберите объект для удаления.
2. Нажмите клавишу Delete на клавиатуре или выберите команду Delete (Удалить) из меню File. Либо выберите Delete из контекстного меню.

Примечание По умолчанию Проводник кладет удаляемые файлы в Recycle Bin (Корзину). Для окончательного удаления файлов нужно очистить Корзину. Для немедленного удаления файлов, минуя корзину, нажмите клавишу Shift и, удерживая ее, нажмите клавишу Delete или выберите Delete из меню File.

Создание папок

1. В панели папок выберите каталог, где будет находиться новая папка.
2. В панели содержимого щелкните правой кнопкой, выберите меню New (Создать), а затем — Folder (Папку). В панели содержимого появится новая папка. Первоначально она будет называться New Folder (Новая папка), и ее имя будет выбрано для редактирования.
3. Измените имя папки и нажмите клавишу Enter.

Просмотр свойств диска

Проводник, папки My Computer и My Network Places позволяют просматривать свойства ваших дисков, включая логические диски, накопители на гибких дисках, сменные, сетевые и компакт-диски.

Просмотреть свойства диска вы можете одним из двух способов:

- щелкнув правой кнопкой значок диска и выбрав Properties;
- выбрав диск, а затем — Properties из меню File.

Некоторые вкладки окна свойств доступны только для разделов NTFS (рис. 12-6). Так, вкладка Security (Безопасность) в NTFS позволяет настроить права доступа, аудита и права владения.

Точное количество вкладок зависит от типа диска (табл. 12-3).

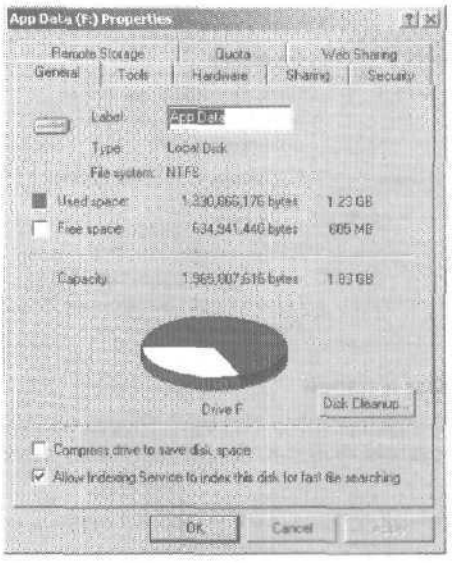


Рис. 12-6. Окно свойств дает краткий обзор диска; количество доступных вкладок зависит от типа диска.

Табл. **12-3.** Доступность и описание вкладок свойств диска.

Вкладка	Доступность	Описание
General (Общие)	Все типы дисков	Обеспечивает обзор конфигурации и объема диска.
Tools (Сервис)	Жесткие, гибкие и сменные диски	Обеспечивает доступ к средствам поиска ошибок, дефрагментации и резервного копирования.
Hardware (Оборудование)	Жесткие, гибкие и сменные диски	Обеспечивает доступ к параметрам устройства и средствам устранения неисправностей.
Sharing (Доступ)	Все локальные диски	Позволяет использовать диск совместно с удаленными пользователями.
Security (Безопасность)	Разделы NTFS	Настраивает права доступа, аудита и владения.
Remote Storage (Внешнее хранилище)	Разделы NTFS	Управляет внешним хранилищем.

Табл. 12-3. *(продолжение)*

Вкладка	Доступность	Описание
Quota (Квота)	Разделы NTFS	Ограничивает дисковое пространство дисков для пользователей.
Web Sharing (Веб-доступ)	Все локальные диски	Позволяет использовать диск совместно с локальным Web-сервером. (Вкладка доступна, когда *в* системе установлены Internet Information Server или Personal Web Server.)

Просмотр свойств файла и папки

Проводник, папки My Computer и My Network Places позволяют просматривать свойства файлов/папок одним из двух способов:

- щелкнув правой кнопкой значок файла/папки и выбрав Properties (Свойства);
- выбрав файл/папку, а затем — Properties из меню File.

Вкладка General (Общие) окна свойств папки на томе NTFS отображает краткую информацию о папке и позволяет назначить атрибуты (рис. 12-7):

- **Read-Only** (Только чтение) показывает, предназначены ли файл/папка только для чтения; вы не сможете изменить или случайно удалить такие файлы/папки;
- **Hidden** (Скрытый) определяет, отображается ли файл в списках; вы можете перекрыть действие этого атрибута, разрешив Проводнику отображать скрытые файлы;
- **Advanced** (Другие) позволяет включить сжатие, шифрование и архивирование для файла.

Доступность вкладок в окне свойств файла/папки зависит от их типа (табл. *12-4),*

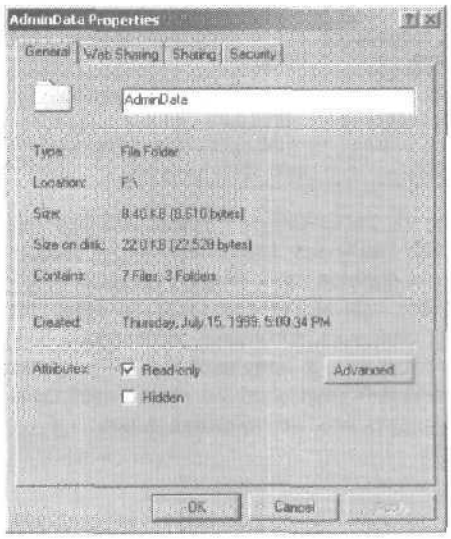


Рис. 12-7. Окна свойств для файла и папки похожи. Доступность вкладок зависит от типа файловой системы и типа файла.

Табл. 12-4. Доступность и описание общих вкладок файла и папки.

Вкладка	Доступность	Описание
General (Общие)	Все файлы и папки	Обеспечивает обзор объекта и позволяет вам устанавливать его атрибуты.
Web Sharing (Веб-доступ)	Все локальные папки	Позволяет использовать папку совместно с локальным Web-сервером. (Вкладка доступна, если в системе установлены Internet Information Services),
Sharing (Доступ)	Все локальные папки	Позволяет использовать папку совместно с удаленными пользователями.
Security (Безопасность)	Файлы и панки NTFS	Настраивает права доступа, аудита и владения.
Summary (Сводка)"	Динамические библиотеки Win32 (DLL) и исполняемые файлы	Позволяет редактировать описание, информацию об авторстве и исправлениях.

Табл. 12-4. *(продолжение)*

Вкладка	Доступность	Описание
Version (Версия)	Динамические библиотеки Win32 (DLL) и исполняемые файлы	Позволяет проверять версию файла, описание, авторские права и другую ключевую информацию.

Примечание Когда вы регистрируете новый тип файлов, могут добавиться или удалиться вкладки свойств. Например, с большей частью файлов изображений вы увидите дополнительные вкладки, где могут содержаться сведения типа ключевых слов, описания, заголовка, источника и т. п. Adobe Photoshop добавляет еще одну вкладку — Photoshop Image, которая показывает миниатюрную копию изображения, что позволит увидеть его, не открывая файл.

Глава 13

Общий доступ к данным, безопасность и аудит

Общий доступ к данным позволяет удаленным пользователям обращаться к сетевым ресурсам: файлам, папкам и дискам. Когда вы делаете общими папку/диск, все их файлы и вложенные папки становятся доступны другим пользователям. Управлять же доступом к определенным файлам и вложенным папкам в общей папке можно только на разделах файловой системы Windows NT (NTFS), списки управления доступом которых служат для предоставления/запрета доступа к файлам/папкам.

Безопасность объекта относится ко всем ресурсам разделов NTFS. Она включает файлы, папки и объекты службы каталогов Active Directory, Обычно только администраторы вправе управлять объектами Active Directory, но вы можете делегировать пользователям полномочия управления объектами. При этом вы открываете им доступ к информации в Active Directory для просмотра и изменения. Разрешения для пользователей задаются в списках управления доступом. Отслеживая доступ к объектам, вы можете тщательно контролировать сетевую активность и обеспечить доступ к ресурсам только авторизованным пользователям.

Общий доступ к папкам на локальных и удаленных системах

Общие ресурсы открыты для доступа удаленных пользователей. Разрешения для общих папок не распространяются на пользователей, регистрирующихся локально па сервере или на рабочей станции, где расположены эти общие папки.

- Для предоставления удаленным пользователям доступа к файлам *в своей сети* служат стандартные разрешения доступа к папкам.

- Для предоставления удаленным пользователям доступа к файлам *из Web* применяется Web-доступ, реализуемый, только если на системе установлены службы Internet Information Services.

Просмотр имеющихся общих ресурсов

Вы можете увидеть общие папки на локальном/удаленном компьютере.

1. В консоли Computer Management (Управление компьютером) подключитесь к нужному компьютеру.
2. В дереве консоли раскройте последовательно узлы System Tools (Системные средства) и Shared Folders (Общие папки), а затем выберите Shares (Общие ресурсы), Будут отбражены текущие общие ресурсы системы (рис. 13-1).

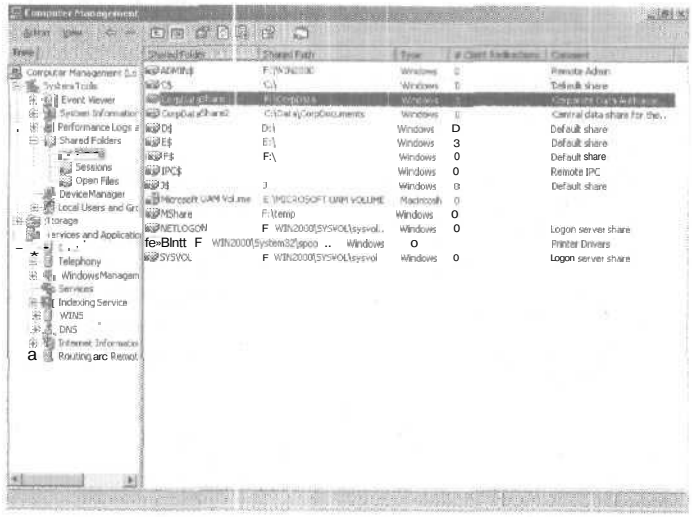


Рис. 13-1. Список доступных ресурсов в узле Shared Folders.

3. В правой панели содержится такая информация:
   - **Shared Folder** (Общая папка) — имя общей папки;
   - **Shared Path** (Общий путь) — полный путь к папке на локальной системе;
   - **Type** (Тип) — тип компьютера, который может использовать этот ресурс;

Примечание Запись «Windows» означает, что все клиенты Microsoft Windows могут обращаться к ресурсу так же, как другие разрешенные клиенты, например пользователи Macintosh. Запись «Macintosh» означает, что к этому ресурсу могут обращаться только клиенты Macintosh.

- **# Client** Redirections (Количество перенаправлений клиентам) — количество клиентов, имеющих доступ к ресурсу в данный момент;
- Comment (Комментарий) — описание ресурса.

Создание общих папок

Microsoft Windows 2000 обеспечивает два способа открытия общего доступа: к локальным папкам (через Проводник Windows) или к локальным и удаленным папкам (через консоль Computer Management).

Computer Management позволяет управлять общими ресурсами с любого компьютера сети. Для создания общих папок на Windows 2000 Server вы должны входить в группы Administrators (Администраторы) или Server Operators (Операторы сервера). Чтобы создать общую папку на Windows 2000 Workstation, нужно быть членом групп Administrators или Power Users (Опытные пользователи).

Общая папка в Computer Management создается так.

1. Щелкните правой кнопкой Computer Management в дереве консоли и выберите Connect To Another Computer (Подключиться к другому компьютеру). Затем выберите нужный компьютер в окне Select Computer (Выбор: Компьютер).
2. В дереве консоли раскройте последовательно узлы System Tools и Shared Folders, а затем выберите Shares. Будут показаны текущие общие ресурсы системы.
3. Щелкнув правой кнопкой Shares, выберите New File Share (Новый общий файл). Откроется мастер Create Shared Folder (Создание общей папки) (рис. 13-2).
4. В поле Folder To Share (Общая папка) наберите локальный путь к папке, к которой вы хотите открыть доступ. Путь должен быть полным, например C:\Data\CorpDocuments. Если вы не знаете полного пути, щелкните Browse (Обзор) и в окне Browse For Folder (Обзор папок) найдите нужную папку.

Совет Если требуемого пути не существует, мастер может создать его. Щелкните Yes (Да), когда появится предложение создать нужную папку.

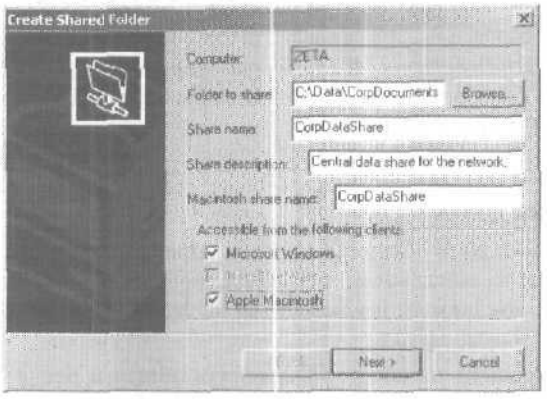


Рис. 13-2. Мастер Create Shared Folder (Создание общей папки) позволяет создать новый общий ресурс на выбранном компьютере. Параметры доступности клиента появляются только при установленных File Services For Macintosh (Файловые службы для Macintosh).

5. Введите имя ресурса. Это имя папки, к которой будут обращаться пользователи. Имена ресурсов должны быть уникальными для каждой системы.

Примечание Компьютеры с MS-DOS и Windows 3.1 могут получить доступ только к ресурсам, имена которых соответствуют стандарту 8.3. Чтобы обеспечить для них доступность ресурса, вы должны соблюдать правило именования 8.3. Например, вместо PrimaryShare лучше использовать имя PRIMARY.SHR или что-то подобное. О правилах именования см. главу 12.

6. Вы можете ввести описание ресурса. Впоследствии, когда вы будете просматривать общие ресурсы на каком-то компьютере, описание будет показано в Computer Management.
7. Дополнительно можно определить типы клиентов, которые будут иметь доступ к компьютеру:
   - Microsoft Windows;

- Novell Netware;
- Apple Macintosh.

Примечание Ресурсы для Apple Macintosh и Novell Netware должны быть созданы на NTFS. File Server For Macintosh — это служба, которая делает файлы доступными пользователям Macintosh. Эти службы нужно установить и запустить, если вы хотите открыть доступ к общим ресурсам пользователям этих систем. Настроить компьютер как файловый сервер позволяет программа Configure Your Server (Настройка сервера): установить дополнительные компоненты поможет мастер.

8. Если в качестве типа клиента выбран Apple Macintosh, вы можете изменить имя ресурса по умолчанию для пользователей Macintosh, набрав новое имя в поле Macintosh Share Name (Имя ресурса Macintosh).
9. Щелкните Next (Далее), а затем настройте базовые разрешения доступа к ресурсу (рис. 13-3); см. раздел «Управление разрешениями доступа к общему ресурсу». Вам доступны следующие параметры.
   - **АИ Users Have Full Control** (Все пользователи имеют полный доступ) дает пользователям полный доступ к ресурсу, т. с. они могут выполнять любые действия с общими файлами/папками: создавать, изменять и удалять их. На разделах NTFS это также дает пользователям право менять разрешения доступа и становиться владельцами файлов/лапок.
   - **Administrators Have Full Control; Other** Users **Have Read-Only Access** (Администраторы имеют полный доступ; остальные имеют доступ только для чтения) дает администраторам полный доступ к ресурсу. Остальные пользователи могут только просматривать файлы и читать данные, но не создавать, изменять или удалять файлы/папки.
   - **Administrators Have Full Control; Other Users Have No Access** (Администраторы имеют полный доступ; остальные не имеют доступа) дает администраторам полный доступ к ресурсу, но запрещает доступ остальным пользователям. Используйте этот параметр, если хотите создать общий ресурс и предоставить пользо-

вателям разрешения доступа позже или если хотите создать административный ресурс.

- **Customize Share And Folder Permissions** (Настроить общий ресурс и разрешения доступа к папке) позволяет настроить доступ для определенных пользователей и групп; обычно это лучший вариант. О настройке разрешений доступа к общему ресурсу см. раздел «Управление разрешениями доступа к общему ресурсу».

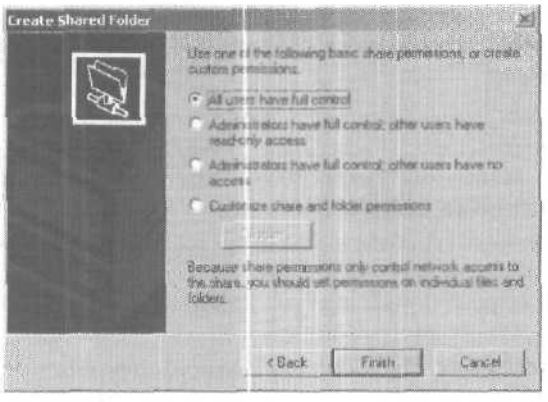


Рис. 13-3. Настройка разрешений доступа к общему ресурсу.

10. Щелкните Finish (Готово).

Примечание Просматривая теперь общие папки в Проводнике Windows, вы увидите на значке папки руку, т. е. папка стала общей. Через Computer Management вы также можете просмотреть общие ресурсы — см. раздел «Общий доступ к папкам на локальных и удаленных системах».

Создание дополнительных общих ресурсов на базе существующего

Отдельным папкам можно сопоставить несколько ресурсов общего доступа, причем каждый может иметь свое имя и набор разрешений доступа. Создавая дополнительные ресурсы на базе существующего, следуйте инструкциям по созданию ресурса предыдущего раздела с такими изменениями:

- в п. 3: присваивая имя ресурсу, убедитесь, что оно отличается от других, ранее присвоенных;

- в п. 6: в описании ресурса объясните, для чего он используется (и чем отличается от других ресурсов для той же папки).

Создание Web-ресурса

Если в системе, на которой вы в данный момент зарегистрированы, установлены службы Internet Information Services (IIS), вы можете создать общие ресурсы, которые будут доступны из Web-обозревателей.

1. В Проводнике правой кнопкой щелкните локальную папку, к которой хотите открыть доступ, и выберите Properties (Свойства).
2. В окне свойств щелкните вкладку Web Sharing (Доступ через веб) (рис. 13-4).

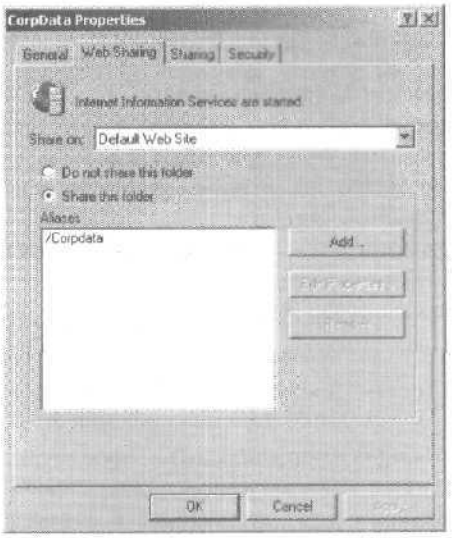


Рис. 13-4. Web-ресурс создается на вкладке Web Sharing.

3. В списке Share On выберите локальный Web-узел, на котором хотите открыть доступ к этой панке,
4. Если это первый общий ресурс для данной папки, щелкните Share This Folder (Предоставить совместный доступ к папке), чтобы открыть окно Edit Alias (рис. 13-5); иначе щелкните Add (Добавить).

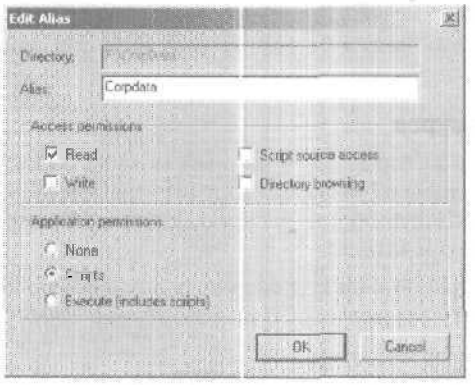


Рис. 13-5. Окно Edit Alias позволяет настроить псевдоним и разрешения доступа для папки.

5. В поле Alias (Псевдоним) введите псевдоним папки. Псевдоним — это имя, которое вы будете использовать для доступа к папке на Web-сервере. Оно должно быть уникальным и не должно конфликтоиать с существующими папками, используемыми Web-сервером. Скажем, если вы наберете псевдоним MyDir, вы сможете обращаться к папке по адресу *http://localhost/MyDir/*.
6. Установите разрешения доступа для папки. Следующие флажки позволяют пользователям Web:
   - Read (Чтение) — читать файлы в папке;
   - Write (Запись) -- записывать файлы в папку;
   - Script Source Access (Доступ к тексту сценария) — получить доступ к исходным текстам сценариев;
   - Directory Browsing (Обзор каталога) — просматривать папку и вложенные в нее подпапки.
7. Установите разрешения для приложений в папке. Вам доступны такие флажки:
   - None (Отсутствуют) запрещает выполнение программ и сценариев;
   - Scripts (Сценарии) позволяет запускать сценарии в этой папке из Web;
   - Execute (Includes Scripts) [Выполнение (включая сценарии)] позволяет выполнять программы и сценарии в этой папке из Web.

8. **Закончив,** щелкните OK.
9. Для дальнейшего ограничения доступа к содержимому общей папки на разделе NTFS настройте разрешения файла/папки (см. раздел «Разрешения доступа к файлам и папкам»).

Примечание Управление доступом к Web-ресурсам осуществляется Web-сервером и Windows 2000. Если у вас проблемы с доступом к ресурсу, проверьте разрешения Web-сервера, а затем разрешения доступа к файлам и папкам Windows 2000.

Управление разрешениями доступа к общему ресурсу

Разрешения доступа устанавливают максимально возможные действия в общей папке. По умолчанию при создании общего ресурса любой пользователь сети имеет полный доступ к содержимому этого ресурса. На разделах NTFS можно задать разрешения доступа к файлам/папкам внутри общей папки для дополнительного ограничения доступа к объектам внутри общей папке и к ней самой. На разделах FAT доступ регулируют только разрешения для самого ресурса.

Виды разрешений доступа к общим ресурсам

Ниже перечислены разрешения доступа к ресурсам по степени ограничения от более жестких к менее.

- No Access (Нет доступа) — доступ к этому ресурсу запрещен.
- Read (Чтение) - с этим разрешением пользователь может:
  - видеть имена файлов и папок;
  - иметь доступ к подпапкам общего ресурса;
  - читать данные и атрибуты файлов;
  - запускать на выполнение программы.
- Change (Изменение) — пользователям разрешено читать данные из папки, а также:
  - создавать файлы и подпапки;
  - изменять файлы;
  - изменять атрибуты файлов и подпапок;
  - удалять файлы и подпапкн.

- **Full Control** (Полный доступ) — пользователи имеют разрешения чтения/изменения, а также дополнительно получают в разделах NTFS возможность:
  - изменять разрешения доступа к файлам/папкам;
  - становиться владельцами файлов/папок.

Примечание Только на разделах NTFS можно установить разрешения доступа к файлам/папкам и права владения файлами/папками.

Вы можете назначить разрешения доступа к общим ресурсам пользователям/группам. Можно назначить разрешения доступа даже неявным группам. О неявных группах см. главу 7.

Просмотр разрешений доступа к общему ресурсу

Вы можете просмотреть разрешения доступа к общему ресурсу.

1. В консоли Computer Management подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли раскройте последовательно узлы System Tools и Shared Folders, а затем выберите Shares.

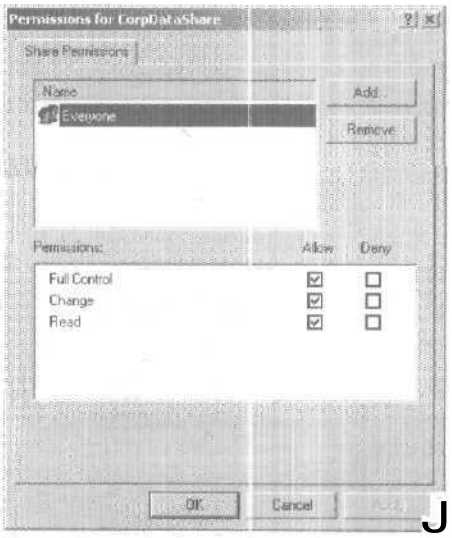


Рис. 13-6. Окно Share Permissions отображает пользователей и группы, имеющие доступ к ресурсу, и тип этого доступа.

3. Правой кнопкой щелкните ресурс, который хотите посмотреть, и выберите Properties.
4. В окне свойств щелкните вкладку Share Permissions (Разрешения для общего ресурса) (рис. 13-6). Теперь вы видите, какие пользователи и группы имеют доступ к этому ресурсу и тип этого доступа.

Настройка разрешений доступа к общему ресурсу

В консоли Computer Management можно добавить разрешения доступа пользователя, компьютера и группы к ресурсу.

1. Правой кнопкой щелкните ресурс, которым хотите управлять, и выберите Properties.
2. В окне свойств щелкните вкладку Share Permissions.
3. Выберите Add. Откроется окно Select Users, Contacts, Computers, Or Groups (Выбор: Пользователи, Контакты, Компьютеры или Группы) (рис. 13-7). Параметры этого окна таковы.
   - Look In (Искать в) — список, позволяющий получить доступ к учетным записям в других доменах. Щелкните Look In для просмотра списка текущего домена,

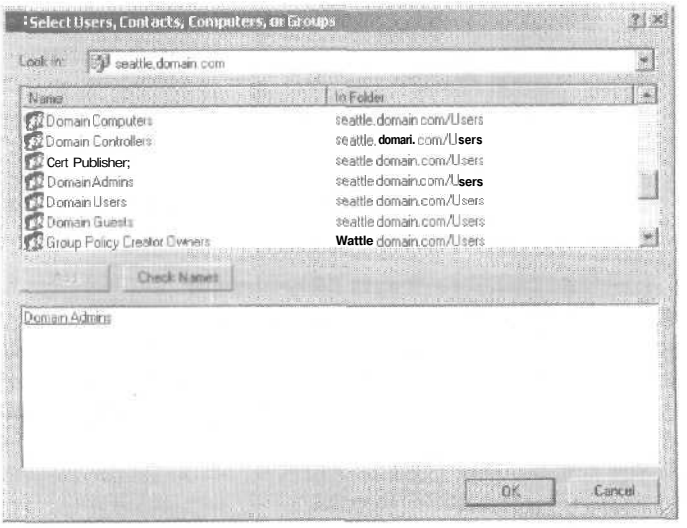


Рис. 13-7. Добавление пользователей и групп к общему ресурсу в окне Select Users, Contacts, Computers, Or Groups.

доверенных доменов и других ресурсов, к которым вы имеете доступ. Выберите Entire Directory (Вся папка) для просмотра всех учетных записей в папке.

Примечание В список Look In попадают только домены, с которыми установлены доверительные отношения. Поскольку в Windows 2000 используется транзитивное доверие, это обычно означает, что все домены в дереве или лесу будут присутствовать в списке.

- **Name** (Имя) — перечень доступных учетных записей в выбранном домене/ресурсе.
- Add (Добавить) — кнопка добавляет выбранные имена в список выбора.
- **Check Names** (Проверить имена) — кнопка подтверждает правильность имен пользователей и групп, внесенных в список выбора. Это полезно, если вы вводили имена вручную и хотите убедиться, что они существуют.

4. Щелкните OK. Пользователи и группы будут добавлены в список имен для общего ресурса.
5. Настройте разрешения доступа для каждого пользователя, контакта, компьютера и группы, выбирая учетную запись и предоставляя/запрещая нужные разрешения. Помните: вы задаете максимально возможные разрешения для конкретного пользователя, контакта, компьютера или группы.
6. Щелкните OK. О назначении дополнительных разрешений безопасности па томе NTFS см. раздел «Разрешения доступа к файлам и панкам».

Изменение существующих разрешений доступа к общему ресурсу

Вы можете изменить разрешения доступа к общему ресурсу, которые вы назначили пользователю, контакту, компьютеру или группе, в окне Share Permissions. В консоли Computer Management сделайте так.

1. Правой кнопкой щелкните ресурс, которым хотите управлять, и выберите Properties.
2. В окне Share Properties щелкните вкладку Share Permissions.

3. В списке Name (Имена) выберите пользователя, контакт, компьютер или группу, разрешения доступа которых вы хотите изменить.
4. Используйте поля в области Permissions (Разрешения) для предоставления/запрета разрешений доступа.
5. Повторите эти действия для других пользователей, контактов, компьютеров или групп; щелкните OK, когда закончите.

Удаление разрешений доступа пользователей и групп к общему ресурсу

Удалить разрешения доступа к общему ресурсу, назначенные пользователям, контактам, компьютерам и группам, можно в окне Share Permissions. Б консоли Computer Management сделайте так.

1. Правой кнопкой щелкните ресурс, которым хотите управлять, и выберите Properties.
2. В окне Share Properties щелкните вкладку Share Permissions.
3. В списке Name выберите пользователя, контакт, компьютер или группу, разрешения доступа которых вы хотите удалить, и выберите Remove (Удалить).
4. Повторите эти действия для других пользователей, контактов, компьютеров или групп, и щелкните OK.

Управление существующими общими ресурсами

Администратору часто придется управлять общими папками.

Понятие о специальных ресурсах

Когда вы устанавливаете Windows 2000. ОС автоматически создает специальные ресурсы. Их также называют *административными* и *скрытыми*. Эти ресурсы призваны облегчить системное администрирование. Вы не можете настроить разрешения доступа к специальным ресурсам — Windows 2000 назначает их сама. Однако вы можете удалить специальные ресурсы, если какие-то из них вам не нужны.

Доступность специальных ресурсов определяют параметры системы. Ниже приведен список и правила использования специальных ресурсов (табл. 13-1).

Табл. 13-1. Специальные **ресурсы, используемые в Windows 2000.**

Имя специального ресурса	Описание	Использование
ADMIN$	**Используется во** время удаленного администрирования системы.	На рабочих станциях и серверах доступ к этому ресурсу имеют члены групп Administrators и Backup Operators (Операторы архива). На контроллерах домена к ним добавляются члены группы Server Operators.
FAX$	Поддерживает сетевые факсы.	Используется клиентами службы FAX при отсылке факсов.
IPC$	Поддерживает именованные каналы во время удаленного IPC-доступа.	Используется программами во время удаленного администрирования и ири просмотре общих ресурсов.
NETLOGON	Поддерживает службу Net Logon,	Используется службой Net Logon при обработке запросов на регистрацию в домене. Все пользователи имеют доступ на чтение.
Microsoft t'AM Volume	Поддерживает службы файлов и печати Macintosh	Используется File Server For Macintosh и Print Server For Macintosh.
PRINT$	Поддерживает общие принтеры,обеспечивая доступ к драйверам принтеров.	Используется общими принтерами. Все пользователи имеют доступ на чтение. Члены групп Administrators, Server Operators и Printer Operators (Операторы печати) имеют полный доступ.
SYSVOL	Поддерживает Active Directory.	Используется для хранения данных и объектов Active Directory.
Driveletter$	**Позволяет** администраторам подключаться к корневой папке диска. Эти ресурсы отображаются, как C$. DS, ES и т. д.	На рабочих станциях и серверах доступ к этому ресурсу имеют члены групп Administrators и Backup Operators. На контроллерах домена к ним добавляются члены группы Server Operators.

Подключение к специальным ресурсам

Имена специальных ресурсов заканчиваются символом «$». Хотя эти ресурсы и не отображаются в Проводнике Windows, администраторы и некоторые операторы могут подключаться к ним. Чтобы подключиться к специальному ресурсу, сделайте так.

1. В Проводнике в меню Tools (Сервис) выберите Map Network Drive (Подключить сетевой диск). Откроется диалоговое окно (рис. 13-8).
2. *В* поле Drive (Диск) выберите свободную букву диска. Эта буква будет служить для доступа к специальному ресурсу.
3. В поле Folder наберите UNC-путь к нужному ресурсу, Например, для доступа к ресурсу C$ на сервере Twiddle нужно ввести **\\TWIDDLE\C$**.
4. Щелкните OK.

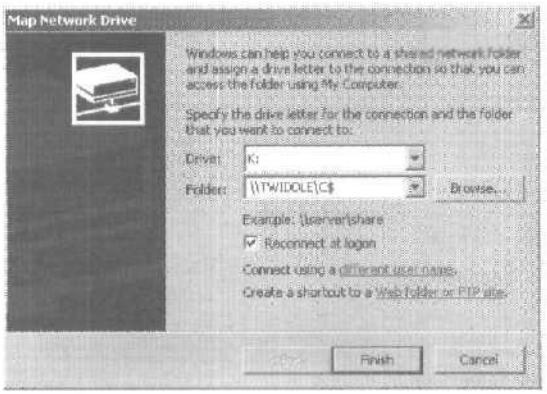


Рис. 13-8. Подключение к специальному ресурсу через диалоговое окно Map Network Drive.

После подключения к специальному ресурсу вы получаете доступ к нему, как к любому другому диску. Поскольку специальные ресурсы защищены, вам не нужно беспокоиться, что обычные пользователи получат доступ к этому ресурсу. Когда вы подключаетесь к ресурсу впервые, вам может быть предложено ввести имя и пароль пользователя.

Просмотр сеансов пользователей и компьютеров

Консоль Computer Management может отследить все подключения к общим ресурсам в системе Windows 2000. Как толь-

ко пользователь/компьютер подключаются к общему ресурсу, подключение отображается в узле Sessions (Сеансы).

Вот как просмотреть подключения к общим ресурсам.

1. В консоли Computer Management подключитесь к компьютеру, на котором создан ресурс.
2. В дереве консоли раскройте последовательно узлы System Tools и Shared Folders, а затем выберите Sessions.
3. Вы можете видеть подключенных к ресурсу пользователей/компьютеры (рис. 13-9).

Рис. 13-9. Просмотр подключений пользователей и компьютеров,

Узел Sessions дает важную информацию о подключениях пользователей и компьютеров:

- **User** (Пользователь) — имена пользователей/компьютеров, подключенных к общим ресурсам; имена компьютеров показаны с суффиксом «$», чтобы отличить их от имен пользователей.
- Computer (Компьютер) — IP-адрес, используемый компьютером;
- **Type** (Тип) — тип используемого компьютера;

- **Open** Files (Открытые файлы) — количество файлов, с которыми пользователь активно работает; более подробную информации вы найдете в узле Open Files;
- Connected Time (Время подсоединения) — время, прошедшее с начала соединения;
- Idle Time (Время простоя) — время, прошедшее с момента, когда соединение использовалось в последний раз;
- Guest (Гость) — регистрировался ли пользователь как гость.

Управление сеансами и общими ресурсами

Прежде чем вы отключите сервер или приложение, работающее на нем, желательно отключить пользователей от общих ресурсов. Вам также может понадобиться отключить пользователей, когда вы собираетесь изменить разрешения доступа или совсем удалить общий ресурс. Еще одна причина отключения пользователей — снятие блокировки файлов. Пользователь отключается от общих ресурсов путем завершения относящихся к нему сеансов.

Завершение отдельных сеансов. Вот как отключить отдельных пользователей от общих ресурсов.

1. В консоли Computer Management подключитесь к компьютеру, на котором создан ресурс.
2. В дереве консоли раскройте последовательно узлы System Tools и Shared Folders, а затем выберите Sessions.
3. Правой кнопкой щелкните нужный пользовательский сеанс и выберите Close Session (Отключить сеанс).
4. Щелкните OK для подтверждения действия.

Завершение всех сеансов. Чтобы отключить от общих ресурсов всех пользователей, сделайте так.

1. В консоли Computer Management подключитесь к компьютеру, на котором создан ресурс.
2. В дереве консоли раскройте последовательно узлы System Tools и Shared Folders, а затем выберите Sessions.
3. Выбрав Disconnect All Sessions (Отключить все сеансы), щелкните OK для подтверждения действия.

Примечание Помните: вы отключаете пользователей от общих ресурсов, а не от домена. Вы можете заставить пользователей завершить **сеанс** после их входа в домен,

только ограничив разрешенное время работы или средствами групповой политики. Так что отключение пользователей от общего ресурса не отключает их от сети.

Управление открытыми ресурсами

Пока пользователь подключен к общему ресурсу, отдельные файлы и объекты ресурса, с которыми он активно работает, отображаются в узле Open Files (Открытые файлы). Узел Open Files может показать файлы, которые пользователь открыл, но не редактирует R данный момент.

Вот как получить доступ к узлу Open Files.

1. В консоли Computer Management подключитесь к компьютеру, на котором создан ресурс.
2. В дереве консоли раскройте последовательно узлы System Tools и Shared Folders, а затем выберите Open Files. Будет показан узел Open Files (рис. 13-10).

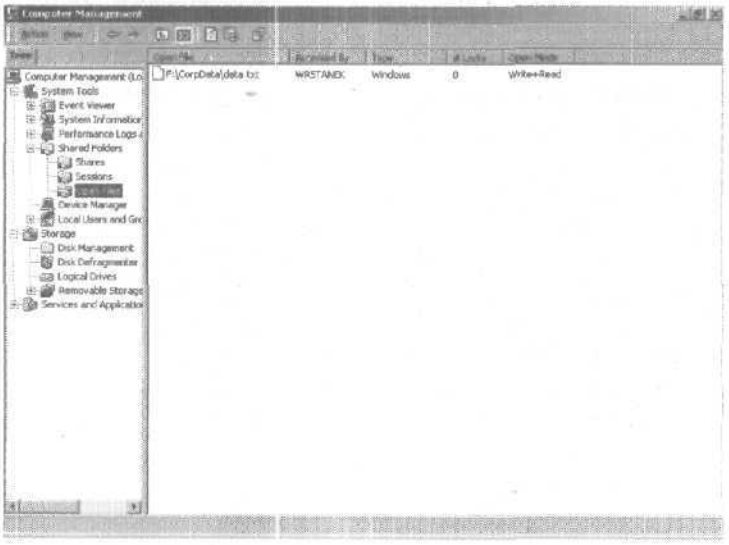


Рис. 13-Ю. Вы можете управлять открытыми ресурсами, используя узел Open Files.

Узел Open Files даст следующую информацию об использовании ресурса:

- **Open File** (Открытый файл) — путь к открытому файлу/папке на локальной системе; может также быть именованным каналом, например \PIPE\spools для буферизации печати;
- **Accessed By** (Пользователь) — имя пользователя, открывшего файл;
- Type (Тип) — тип используемого компьютера;
- **# Locks** (Блокир.) — количество блокировок ресурса;
- **Open Mode** (Режим открытия) — использовавшийся при открытии ресурса режим доступа: чтения, записи или чтения-записи.

Закрыть открытый файл в ресурсах компьютера можно так.

1. В "консоли Computer Management подключитесь к компьютеру, с которым хотите работать.
2. В дереве консоли раскройте последовательно узлы System Tools и Shared Folders, а затем выберите Open Files.
3. Правой кнопкой щелкните открытый файл и выберите Close Open File (Закрыть открытый файл).
4. Щелкните OK для подтверждения действия.

Закрыть все открытые файлы в ресурсах компьютера можно так.

1. В консоли Computer Management подключитесь к компьютеру, с которым хотите работать.
2. В дереве консоли раскройте последовательно узлы System Tools и Shared Folders, а затем выберите Open Files.
3. Выбрав Disconnect All Open Files (Отключить все открытые файлы), щелкните OK для подтверждения действия.

Прекращение общего доступа к файлам и папкам

1. В консоли Computer Management подключитесь к компьютеру, на котором создан ресурс и раскройте узел Shares.
2. Правой кнопкой щелкните ресурс, который хотите удалить, и выберите Stop Sharing (Прекратить общий доступ). Щелкните OK для подтверждения действия.

Внимание! Никогда не удаляйте папку, содержащую общие ресурсы, без предварительного прекращения доступа к этим ресурсам. Если вы забудете прекратить доступ, Windows 2000 попытается восстановить доступ при следу-

ющем запуске компьютера, результатом чего будет запись об ошибке в системном журнале.

Подключение к сетевым дискам

Пользователи могут подключаться к сетевым дискам и общим ресурсам, доступным в сети. Эти соединения выглядят как сетевые диски, к которым пользователи обращаются так же, как к другим дискам в своих системах,

Примечание Когда пользователи подключаются к сетевым дискам, на них действует не только набор разрешений доступа к общим ресурсам, но и разрешения доступа к файлам/папкам Windows 2000. Различия в этих наборах разрешений обычно являются причиной того, что пользователи не могут получить доступ к отдельным файлам/подпапкам на сетевом диске.

Подключение сетевого диска

В Windows 2000 подключение к сетевому диску осуществляется путем проекции. Для этого применяются процедуры, зависящие от конкретной ОС.

Вот как подключиться к общему ресурсу Windows 2000.

1. После регистрации пользователя запустите Проводник на его компьютере.
2. В меню Tools (Сервис) выберите Map Network Drive (Подключить сетевой диск). Откроется диалоговое окно Map Network Drive.
3. В поле Drive (Диск) можно создать сетевой диск для общего ресурса. Выберите свободную букву диска для создания сетевого диска, к которому можно будет обращаться через Проводник, и папку My Computer (Мой компьютер). Можно выбрать None для создания сетевого диска без назначения буквы. Этот диск открывается и собственном окне Проводника Windows и недоступен через My Computer.
4. В поле Folder наберите UNC-путь к нужному ресурсу. Например, для доступа к ресурсу DOCS на сервере ROMEO нужно ввести **\\ROMEO\DOCS.** Если вы не знаете точного места размещения ресурса, щелкните Browse (Обзор) для поиска доступных ресурсов.

5. Если вы хотите, чтобы сетевой диск автоматически подключался в последующих сеансах, выберите Reconnect At Logon (Автоматически подключать при входе в систему). Иначе снимите этот флажок и дважды щелкните сетевой диск, который хотите подключить.
6. Для подключения от имени пользователя, отличного от того, под которым вы регистрировались и системе, щелкните Different User Name (под другим именем) и введите имя пользователя и пароль.
7. Щелкните OK.

Совет В других ОС, например Novell Netware, можно использовать UNC из командной строки:

```
Net Use K: \\Server1\Public
```

Если хотите сделать это подключение постоянным, добавьте /Persistent:yes в конце:

```
Net Use K: \\Server1\Public /Persistent:yes
```

Тогда система будет пытаться получить доступ к папке Public на сервере Server1 при каждом входе в систему.

Отключение сетевого диска

Сетевой диск отключается так.

1. После регистрации пользователя запустите Проводник Windows на компьютере пользователя.
2. Б меню Tools выберите Disconnect Network Drive (Отключить сетевой диск). Откроется диалоговое *окно* Disconnect Network Drive.
3. Выберите нужный диск и щелкните OK.

Управление объектами, правами владения и наследованием

В Windows 2000 реализован объектный подход к описанию ресурсов и управлению разрешениями доступа. Объекты, описывающие ресурсы, определяются в разделах NTFS и в Active Directory. На разделах NTFS можно настраивать разрешения доступа к файлам/папкам, а средствами Active Directory — разрешения доступа к другим объектам, таким как пользователи, контакты, компьютеры и группы.

Объекты и диспетчеры объектов

Независимо от того, где определен объект: в разделе NTFS или в Active Directory, - у каждого типа объектов свой диспетчер и базовые средства управления. Диспетчер объектов управляет параметрами объекта и разрешениями доступа к нему. Базовые средства управления — предпочтительные инструменты работы с объектами. Объекты, их диспетчеры и средства управления перечислены ниже (табл. 13-2).

Табл. 13-2. Объекты Windows 2000.

Тип объекта	Диспетчер объекта	Средство управления
Файлы и папки	NTFS	Проводник
Общие ресурсы	Служба Server	Проводник, консоль Computer Management
Записи реестра	Реестр Windows	Редактор реестра (regedit)
Службы	Контроллеры служб	Набор средств настройки безопасности (Security Configuration Tool Set)
Принтеры	Спулер печати	Папка Printers (Принтеры) в Control Panel (Панель управления)

Владение и передача объектов

В Windows 2000 владелец объекта не обязательно является его создателем, но именно владелец объекта полностью управляет им. Владелец объекта может разрешать доступ и давать другим пользователям право становиться владельцами объекта.

Администратор вправе завладеть любыми объектами в сети. За счет этого для авторизованных администраторов нельзя заблокировать файлы, папки, принтеры и другие ресурсы. Но став владельцем файлов, вы (в большинстве случаев) не можете вернуть их предыдущему владельцу. Это предотвращает возможность администратора получить доступ к файлу, а затем скрыть этот факт.

Порядок назначения прав владения изначально определяется местом размещения создаваемого ресурса. Обычно группа Administrators является текущим владельцем объекта, а его действительный создатель имеет право стать владельцем.

Передать владение можно такими способами.

- Если администраторы изначально назначаются владельцами, создатель объекта может стать владельцем при

условии, что он сделает это прежде, чем кто-либо другой станет владельцем.

- Текущий владелец может предоставить разрешение Take Ownership (Смена владельцем) другим пользователям, разрешив им становиться владельцами объекта.
- Администратор может стать владельцем объекта, взяв его под свое управление.

Вот как сменить владельца объекта.

1. Запустите средство управления этим объектом. Например, если хотите работать с файлами/папками, запустите Проводник.
2. Правой кнопкой щелкните объект, владельцем которого хотите стать.
3. Выберите Properties, а затем в окне свойств — вкладку Security (Безопасность).
4. Щелкнув кнопку Advanced (Дополнительно), откройте диалоговое окно Access Control Settings (Параметры управления доступом). Затем выберите вкладку Owner (Владелец) (рис. 13-11).

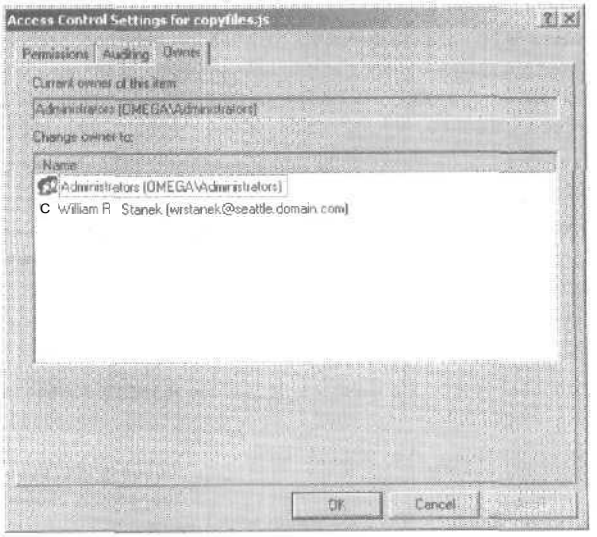


Рис. 13-11. На вкладке Owner можно сменить владельца файла.

5. Выберите имя нового владельца к списке Change Owner To (Изменить владельца на), а затем — OK.

Наследование объектов

Объекты определяются с использованием структуры родитель — потомок. Родительский объект — объект верхнего уровня. Дочерний определяется в иерархии ниже родительского. Например, папка C:\ является родительской для папок C:\data и C:\backups. Любые подпапки, созданные в C:\data или C:\backups являются дочерними для этих папок и внучатыми для C:\.

Дочерние объекты могут наследовать разрешения от родительских объектов. Фактически все объекты Windows 2000 по умолчанию создаются с разрешением наследования. Это значит, что дочерние объекты автоматически наследуют разрешения родительских, поэтому разрешения родительского объекта управляют доступом к дочернему. Чтобы изменить разрешения дочернего объекта:

- отредактируйте разрешения родительского объекта;
- остановите наследование разрешений от родительского объекта, а затем назначьте разрешения для дочернего;
- выберите противоположное значение разрешения для перекрытия унаследованного, например, если родитель предоставляет какое-то разрешение, запретите его для дочернего объекта.

Вот как запустить/остановить наследование разрешений от родительского объекта.

1. Запустите средство управления для данного объекта. Например, если хотите работать с файлами/папками, запустите Проводник.
2. Правой кнопкой щелкните объект, с которым хотите работать.
3. В меню выберите Properties, а затем в окне свойств - вкладку Security.
4. Щелкнув кнопку Advanced, откройте диалоговое окно Access Control Settings.
5. На вкладке Permission (Разрешения) установите/снимите флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект),

Разрешения доступа к файлам и папкам

В разделах NTFS вы можете настраивать разрешения безопасности для файлов и папок. Эти разрешения позволяют/запрещают доступ к файлам/папкам. Разрешения безопасности можно просмотреть.

1. В Проводнике правой кнопкой щелкните файл/папку, с которыми хотите работать.
2. В меню выберите Properties, а затем *и* окне свойств - вкладку Security.
3. В списке Name выберите пользователя, контакт, компьютер и группу, разрешения которых вы хотите видеть. Если разрешения затенены, они наследуются от родительского объекта.

Понятие разрешений доступа к файлам и папкам

Ниже приведены базовые разрешения, которые вы можете назначить файлу и папке (табл. 13-3). Разрешения файла: Full Control (Полный доступ). Modify (Изменение), Read & Execute (Чтение и выполнение), Read (Чтение) и Write (Запись). Разрешения папки: Full Control, Modify, Read & Execute, List Folder Contents (Список содержимого папки), Read и Write.

Когда вы работаете с разрешениями файлов/папок, учтите:

- Read — единственное разрешение, необходимое для выполнения сценариев. Разрешение Execute (Выполнение) не требуется;
- Read требуется для доступа к ярлыкам и их целевым объектам;
- предоставляя пользователю разрешение записи в файл, но не его удаления, нельзя предотвратить удаление пользователем содержимого файла — пользователь по-прежнему может удалить содержимое файла;
- имея полный доступ к папке, пользователь может удалять файлы в ней независимо от разрешений на сами эти файлы.

Базовые разрешения создаются комбинацией специальных разрешений в логических группах. Ниже показаны специальные разрешения, используемые при создании базовых разрешений для файлов (табл. 13-4). Используя дополнительные параметры разрешения, вы можете назначать специальные разрешения индивидуально. При изучении специальных разрешений учтите следующее.

- Доступ пользователю должен быть предоставлен явно, иначе доступ ему запрещен.
- Действия, которые может выполнять пользователь, являются суммой всех разрешений, назначенных ему и всем группам, членом которых он является. Например, пользователь GeorgeJ имеет доступ на чтение, кроме того, он является членом группы Techies, которая имеет право изменения. В итоге GeorgeJ будет иметь право изменения. Если Techies будут включены в группу Administrators, которая имеет полный доступ, GeorgeJ также получит полный доступ к этому файлу.

Табл. 13-3. Разрешения файлов и папок в **Windows 2000.**

Разрешение	Позволяет для папок	Позволяет для файлов
Read (Чтение)	Просмотр и получение списка файлов и подпапок	Просмотр/доступ к содержимому файла
Write (Запись)	Добавление файлов и подпапок.	Запись в файл
Read & Execute (Чтение и выполнение)	Просмотр и получение списка файлов и подпапок, а также исполнение файлов (наследуется файлами и папками)	Просмотр/доступ к содержимому файла, а также исполнение файла
List Folder Contents (Список содержимого нанки)	Просмотр и получение списка файлов и подпапок, а также исполнение файлов (наследуется только папками)	—
Modify (Изменение)	Чтение и запись файлов и подпапок, удаление папки	Чтение, запись и удаление файла
Full Control (Полный доступ)	Чтение, запись, изменение и удаление файлов и подпапок	Чтение, запись, изменение и удаление файла

Ниже перечислены специальные разрешения, используемые для создания базовых разрешений для папок (табл. 13-5). При изучении специальных разрешений учтите следующее.

- Устанавливая разрешения для родительской папки, вы можете заставить все файлы и подпапки внутри этой папки унаследовать ее разрешения: выберите Reset Permissions On All Child Objects And Enable Propagation Of Inheritable

Permissions (Сбросить разрешения всех дочерних объектов и разрешить перенос наследуемых разрешений).

- Файлы, создаваемые в папках, наследуют некоторые параметры разрешения. Эти параметры показаны как стандартные разрешения файла.

Табл. 13-4. Специальные разрешения для файлов.

Специальные Разрешения	Full Control	Modify	Read & Execute	Read	Write
Обзор папок / Выполнение файлов	X	X	X		
Получение списка содержимого папки / Чтение данных	X	X	X	X	
Чтение атрибутов	X	X	X	X	
Чтение расширенных атрибутов	X	X	X	X	
Создание файлов / Запись данных	X	X			X
Создание папок / Добавление данных	X	X			X
Запись атрибутов	X	X			X
Запись расширенных атрибутов	X	X			X
Удаление подпапок и файлов	X				
Удаление	X	X			
Разрешения на чтение	X	X	X	X	X
Разрешения на изменение	X				
Смена владельца	X				

Табл. 13-5. Специальные разрешения для папок.

Специальные Разрешения	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Обзор папок /	X	X	X	X		
Получение списка содержимого пайки / Чтение данных	X	X	X	X	X	
Чтение атрибутов	X	X	X	X	X	
Чтение расширенных атрибутов	X	X	X	X	X	
Создание файлов / Запись данных	X	X				X
Создание папок / Добавление данных	X	X				X

Табл. 13-5. *(продолжение)*

Специальные Разрешения	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Запись атрибутов	X	X				X
Запись расширенных атрибутов	X	X				X
Удаление подпапок и файлов	X					
Удаление	X	X				
Разрешения па чтение	X	X	X	X	X	X
Разрешения на изменение	X					
Смена владельца	X					

Настройка разрешений для файла и папки

1. В Проводнике правой кнопкой щелкните файл/папку, с которыми хотите работать.
2. В появившемся меню выберите Properties, а затем **в окне** свойств — вкладку Security (рис. 13-12).

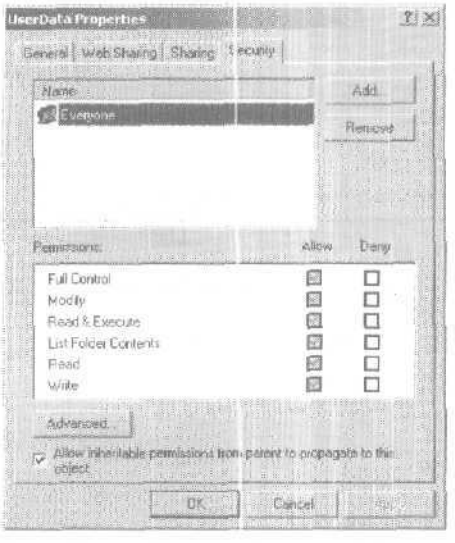


Рис. 13-12. Вкладка Security позволяет настроить базовые разрешения для файла/папки.

3. Пользователи/группы, которые уже имеют доступ к файлу/папке, перечислены в списке Name. Вы можете изменить разрешения для этих пользователей/групп:
   - выберите пользователя/группу, разрешения которых хотите изменить;
   - в списке Permissions предоставьте/запретите разрешения доступа.

Совет Наследуемые разрешения затенены. Если вы хотите перекрыть наследуемое разрешение, выберите противоположное значение.

4. Чтобы задать разрешения доступа для дополнительных пользователей, контактов, компьютеров/групп, щелкните Add. Появится диалоговое окно Select Users, Computers, Or Groups (рис. 13-13).

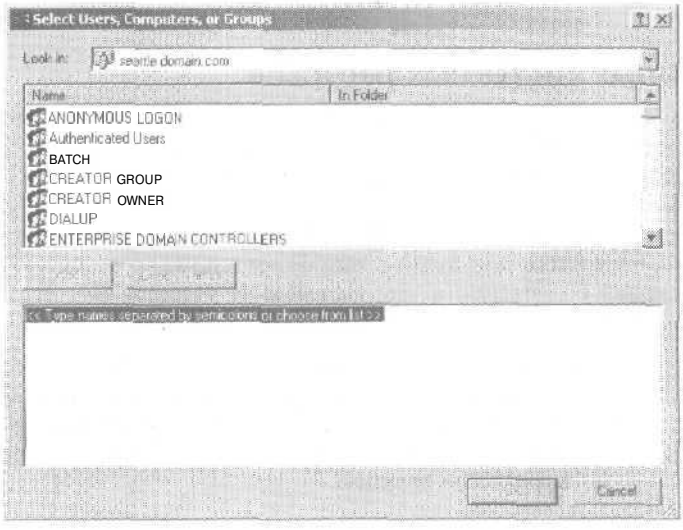


Рис. 13-13. Выберите пользователей, компьютеры/группы, которым нужно предоставить/запретить доступ.

5. В этом окне имеются следующие поля.
   - **Look In** — этот список позволяет получить доступ к учетным записям в других доменах. Щелкните Look In для просмотра списка текущего домена, доверенных доменов и других ресурсов, к которым вы имеете до-

ступ. Выберите Entire Directory (Вся папка) для просмотра всех учетных записей в Active Directory.

- **Name** — здесь перечислены учетные записи в выбранном домене/ресурсе.
- Add — эта кнопка добавляет выбранные имена в список выбора.
- **Check Names** — эта кнопка подтверждает правильность имен пользователей и групп, внесенных в список выбора. Это удобно, если вы вводили имена вручную и хотите убедиться, что они существуют.

6. В списке Name выберите нужных пользователя, компьютер или группу, а затем используйте поля в области Permissions для предоставления/запрета разрешений доступа. Повторите для других пользователей, компьютеров или групп.
7. Щелкните OK, когда закончите.

Аудит системных ресурсов

Аудит — лучший способ проследить, что случилось с вашей системой Windows 2000. Вы можете применять аудит для сбора информации по использованию ресурсов, такой как доступ к файлам, регистрация в системе и изменения системных настроек. Как только произойдет событие, которое вы настроили для аудита, оно будет записано в системный журнал безопасности, где вы сможете увидеть его. Журнал безопасности доступен в консоли Event Viewer.

Примечание Для большей части изменений аудита вам понадобится регистрироваться под учетной записью из группы Administrators или иметь разрешение Manage Auditing And Security Log (Управление аудитом и журналом безопасности) в групповой политике.

Настройка политик аудита

Политики аудита — важный фактор обеспечения безопасности и целостности системы. Почти каждая компьютерная система в сети должна быть настроена для протоколирования определенных параметров безопасности. Политики аудита настраиваются с применением групповой политики: вы можете задать политики аудита для всего сайта, домена или

организационного подразделения (ОП). Вы также можете настроить политики для отдельной рабочей станции/сервера.

Открыв контейнер групповой политики, настройте политику аудита.

1. Доступ к узлу Audit Policy (Политика аудита) можно получить, последовательно спускаясь по дереву консоли (рис. 13-14). Раскройте поочередно Computer Configuration (Конфигурация компьютера), Windows Settings (Конфигурация Windows), Security Settings (Параметры безопасности) и Local Policies (Локальные политики). Затем выберите Audit Policy.

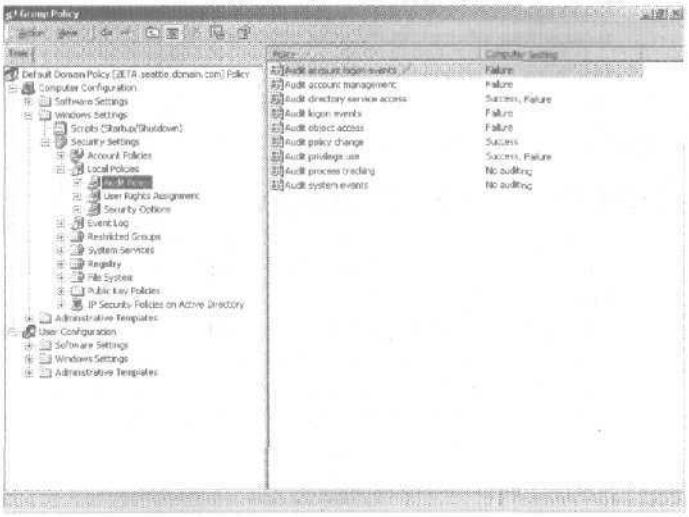


Рис. 13-14. Настройка политики аудита с использованием узла Audit Policy в групповой политике.

2. Параметры аудита перечислены ниже.
   - Audit Account Logon Events (Аудит регистрации учетных записей в системе) отслеживает события, относящиеся к регистрации и окончанию работы пользователя в системе.
   - Audit Account Management (Аудит управления учетными записями) отслеживает управление учетными записями посредством Active Directory Users And Computers. События генерируются каждый раз, когда учет-

ные записи пользователя, компьютера или группы создаются, изменяются или удаляются.

- Audit Directory Service Access (Аудит доступа к службе каталогов) отслеживает доступ к Active Directory. События генерируются каждый раз, когда пользователи/компьютеры получают доступ к каталогу.
- Audit Logon Events (Аудит событий входа в систему) отслеживает события, связанные с регистрацией пользователя, окончанием сеанса работы и удаленными соединениями с сетевыми системами.
- Audit Object Access (Аудит доступа к объектам) отслеживает использование системных ресурсов: файлов, каталогов, общих ресурсов, принтеров и объектов Active Directory.
- Audit Policy Change (Аудит изменений политики) отслеживает изменения разрешений доступа пользователей, аудита и доверительных отношений.
- Audit Privilege Use (Аудит использования привилегий) отслеживает применение разрешений доступа и привилегий пользователя типа права резервного копирования файлов и каталогов.

Примечание Политика аудита привилегий не отслеживает события, относящиеся к системному доступу, такие как использование права интерактивного входа/разрешения доступа к компьютеру из сети. Эти события отслеживаются аудитом регистрации пользователя.

- Audit Process Tracking (Аудит отслеживания процессов) отслеживает системные процессы и ресурсы, ими используемые.
- Audit System Events (Аудит системных событий) отслеживает запуск, выключение и перезагрузку системы, а также действия, влияющие на безопасность системы или на журнал безопасности.

3. Для настройки политики аудита дважды щелкните ее элемент или щелкните его правой кнопкой и выберите Security. Откроется окно свойств этой политики.
4. Выберите Define These Policy Settings, а затем пометьте флажок Success (Успех) либо Failure (Отказ) или оба сразу. Включение Success протоколирует успешные события,

такие как удачные попытки входа в систему. Failure - события отказа, такие как неудачные попытки входа.

5. Щелкните OK, когда закончите.

Аудит файлов и папок

Если вы настроили групповую политику, включив параметр Audit Object Access (Аудит доступа к объектам), вы можете задать уровень аудита для отдельных папок/файлов. Аудит этого типа доступен только на томах NTFS.

Аудит файла/пайки настраивается так.

1. В Проводнике щелкните правой кнопкой файл/папку, для которых нужно включить аудит, и выберите Properties.
2. На вкладке Security щелкните Advanced.
3. В окне Access Control Settings выберите вкладку Auditing (рис. 13-15).

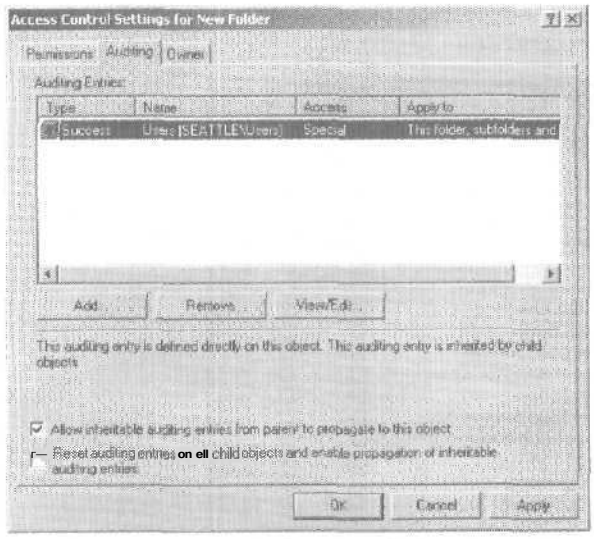


Рис. 13-15. На вкладке Auditing можно настроить политики аудита отдельных файлов/папок.

4. Если вы хотите наследовать параметры аудита от родительского объекта, выберите Allow Inheritable Auditing Entries From Parent To Propagate To This Object (Перс-

носить наследуемые от родительского объекта элементы аудита на этот объект).

5. Если вы хотите, чтобы дочерние объекты текущего объекта наследовали его параметры, выберите Reset Auditing Entries On All Child Objects And Enable Propagation Of Inheritable Auditing Entries (Сброс элементов аудита всех дочерних объектов и разрешение переноса наследуемых элементов аудита).
6. В списке Auditing Entries (Элементы аудита) выберите пользователей, группы или компьютеры, чьи действия вы желаете отслеживать с помощью аудита. Чтобы удалить учетную запись, выберите ее в списке Auditing Entries и щелкните Remove (Удалить).
7. Чтобы добавить определенные учетные записи, щелкните Add, а затем в окне Select Users, Contacts, Computers, Or Groups укажите имя учетной записи. Щелкнув OK, вы увидите диалоговое окно Auditing Entry For (Элемент аудита для) (рис.13-16).

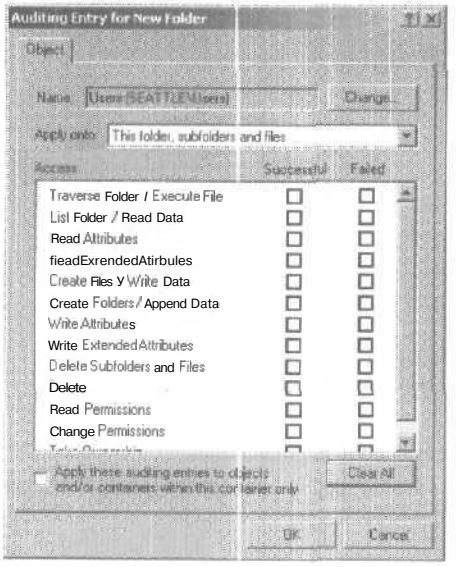


Рис. 13-16. В окне Auditing Entry For задайте элементы аудита для пользователя, контакта, компьютера или группы.

Примечание Для отслеживания с помощью аудита действий всех пользователей служит специальная группа Everyone. Иначе выберите группы пользователей или отдельных пользователей, к которым хотите применить аудит.

8. В списке Apply Onto (Применять) можно определить, где применять аудит объектов.
9. Выберите флажки Successful (Успешное), Failed (Неудачное) или оба сразу, для каждого из событий, к которым хотите применять аудит. Successful протоколирует успешные события, типа успешного чтения файла, Failed - неудачные события, например неудавшееся удаление файла. События, для которых вы можете использовать аудит, — те же, что и специальные разрешения (табл. 13-5), за исключением того, что нельзя отслеживать средствами аудита синхронизацию автономных файлов и панок.
10. Выберите OK, когда закончите. Повторите описанный процесс для аудита других пользователей, групп или компьютеров.

Аудит объектов Active Directory

Если в групповой политике включен параметр Audit Directory Service Access (Аудит доступа к службе каталогов), вы можете задать уровень аудита для объектов Active Directory. Это позволяет точно управлять наблюдением за использованием объекта.

Аудит объекта настраивается так.

1. В консоли Active Directory Users And Computers найдите контейнер объекта.
2. Правой кнопкой щелкните объект, для которого будет применяться аудит, и выберите Properties.
3. На вкладке Security щелкните Advanced.
4. В окне Access Control Settings выберите вкладку Auditing. Если вы хотите наследовать параметры аудита от родительского объекта, выберите Allow Inheritable Auditing Entries From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта элементы аудита на этот объект).

5. В списке Auditing Entries можно выбрать пользователей, группы или компьютеры, чьи действия вы желаете отслеживать с помощью аудита. Чтобы удалить учетную запись, выберите ее в списке Auditing Entries и щелкните Remove.
6. Чтобы добавить определенные учетные записи, щелкните Add, а затем в окне Select Users, Contacts, Computers, Or Groups укажите имя учетной записи. Когда вы нажмете OK, появится диалоговое окно Audit Entry For (Элемент аудита для).
7. Используйте список Apply Onto, чтобы указать, где применять аудит объектов.
8. Выберите флажки Successful, Failed или оба сразу для каждого из событий, которые хотите отслеживать.
9. Щелкните OK, когда закончите. Повторите описанный процесс для аудита других пользователей, групп или компьютеров.

Глава 14

Архивирование и восстановление данных

Данные — сердце компании. Ваша задача — защитить их. Для этого вы должны составить план архивации и восстановления защиты корпоративных данных. Архивация файлов может защитить их от случайной потери, отказа БД, сбоев оборудования и даже стихийных явлений. Администратор обязан выполнять архивацию и хранить архивы в безопасном месте.

Разработка плана архивации и восстановления

Файлы могут быть удалены в любой момент, важные данные — испорчены, стихийные бедствия способны обратить ваш офис в руины. Разработав план архивации и восстановления, вы защитите данные.

Понятие плана архивации

Создание и внедрение плана архивации и восстановления информации требует времени. Вам надо определить, какие данные требуют архивации, как часто проводить архивацию и т. п. При создании плана ответьте на следующие вопросы,

- **Насколько** важны данные? Этот критерий поможет решить, как, когда и какую информацию сохранять. Для критичной информации, например баз данных, нужно создать избыточные архивные наборы, которые разделяют процесс архивации на *несколько* периодов. Для менее важной, такой как пользовательские файлы, нет нужды разрабатывать подробный план архивации, однако вы должны регулярно сохранять и иметь возможность легко ее восстановить.

- **Какой тип информации содержат данные?** Тип информации поможет определить необходимость архивации данных: как и когда данные должны быть сохранены.
- **Как часто изменяются данные?** Частота изменения может повлиять на *выбор* частоты архивирования данных. Например, ежедневно меняющиеся данные надо сохранять каждый день.
- Как часто **приходиться восстанавливать данные?** Время — важный фактор при создании плана архивации. В критичных к скорости системах нужно проводить архивацию очень быстро.
- **Есть ли у вас оборудование для проведения** архивации? Для своевременной архивации вам понадобится несколько архивирующих устройств и несколько наборов носителей. Аппаратные средства архивации включают ленточные накопители (это наименее дорогой, но и самый медленный тип носителя), оптические диски и съемные дисковые накопители.
- **Кто будет** отвечат . за **выполнение плана архивации и восстановления данных?** Идеальный вариант — кто-то один будет разрабатывать план архивации и восстановления. Он же может выполнять архивацию и восстановление.
- **Какое время оптимально для архивации?** Архивация в период наименьшей загрузки системы пройдет быстрее, Но вы нс всегда можете провести архивацию в удобные часы. Поэтому с особой осторожностью архивируйте ключевые данные.
- **Нужно ли сохранять архивы вне офиса?** Хранение архивов вне офиса — важный фактор на случай стихийного бедствия. Вместе с архивами сохраните и копии ПО для установки или переустановки ОС.

Типы архивации

Способ архивации файлов зависит от типа сохраняемых данных, от удобства их восстановления и т. п.

Если вы посмотрите на свойства файла или каталога в Windows Explorer (Проводник), то увидите атрибут Archive (Архивный). Он указывает, можно ли данный файл/каталог архивировать. Если атрибут включен, то файл/каталог, воз-

можно, нуждается в архивации. Основные типы архивации таковы.

- **Обычная/полная архивация.** Все выделенные файлы архивируются независимо от значения атрибута архива, После архивации файла атрибут архива сбрасывается. Если затем файл изменяется, включается атрибут архива, показывая, что файл нуждается в архивации.
- **Копирующая архивация.** Все выделенные файлы архивируются независимо от значения атрибута архива. В отличие от обычной архивации атрибут архива не изменяется. Это позволяет затем выполнять архивацию другого типа.
- **Разностная архивация.** Создает архивные копии файлов, которые были изменены со времени последней обычной архинации. Наличие атрибута архива показывает, что файл был модифицирован. Только файлы с этим атрибутом будут архивированы. Но атрибут архива при этом не изменяется. Это позволяет затем выполнять архивацию другого типа.
- **Добавочная архивация.** Создает архивные копии файлов, которые были изменены со времени последней обычной или добавочной архивации. Атрибут архива показывает, что файл был модифицирован. Только файлы с этим атрибутом будут архивированы. После архивации файлов атрибут архива сбрасывается. Если файл был изменен, для него включается атрибут архива, показывая, что файл требует архивации.
- **Ежедневная архивация.** Сохраняются файлы, измененные за прошедший день. Этот тип архивации не изменяет атрибутов архива файлов.

Вы можете выполнять полную архивацию еженедельно и вдобавок к этому ежедневную, разностную и добавочную архивацию. Вы также можете создать расширенный архивный набор для ежемесячных и ежеквартальных архивов, которые будут включать в себя нерегулярно архивируемые файлы.

Совет Бывает, проходят недели и месяцы прежде чем кто-нибудь обнаружит, что пропал нужный файл или источник данных. Поэтому, планируя ежемесячные или ежеквартальные архивы, не забудьте, что вам может потребоваться восстановить и устаревшие данные.

Разностная и добавочная архивации

Различие между разностной и добавочной архивациями очень существенно (табл. 11-1). При разностной архивации вы сохраняете все файлы, которые были изменены с момента последней полной архивации (т. е. размер разностного архива будет со временем расти). При добавочной архивации вы сохраняете файлы, измененные с момента последней полной или добавочной архивации (т, е. добавочный архив, как правило, гораздо меньше полного).

Табл. 14-1. Технологии добавочной и разностной архивации.

День недели	Еженедельная полная архивация с ежедневной разностной архивацией	Еженедельная полная архивация с ежедневной добавочной архивацией
Воскресенье	Выполнена полная архивация.	Выполнена полная архивация.
Понедельник	Разностный архив содержит все изменения, происшедшие с воскресенья.	Добавочный архив содержит все изменения, происшедшие с воскресенья.
Вторник	Разностный архив содержит все изменения, происшедшие с воскресенья.	Добавочный архив содержит все изменения, происшедшие с понедельника.
Среда	Разностный архив содержит все изменения, происшедшие с воскресенья.	Добавочный архив содержит все изменения, происшедшие со вторника.
Четверг	Разностный архив содержит все изменения, происшедшие с воскресенья.	Добавочный архив содержит все изменения, происшедшие со среды.
Пятница	Разностный архив содержит все изменения, происшедшие с воскресенья.	Добавочный архив содержит все изменения, происшедшие с четверга.
Суббота	Разностный архив содержит все изменения, происшедшие с воскресенья.	Добавочный архив содержит все изменения, происшедшие с пятницы.

Определив, какие данные и как часто архивировать, можно выбрать аппаратные средства архивации и необходимые носители.

Выбор архивных устройств и носителей

Инструментов для архивации данных множество. Одни - быстрые и дорогие, другие — медленные и надежные. Выбор подходящего для организации зависит от многих факторов.

- Емкость — количество регулярно архивируемых данных. Справится ли оборудование с нагрузкой в отведенное время?
- Надежность аппаратных средств и носителей. Можете ли вы пожертвовать надежностью ради экономии или скорости?
- Расширяемость решения. Удовлетворит ли ваше решение потребностям расширившейся организации?
- Скорость архивации и восстановлении. Можете ли вы пожертвовать скоростью ради снижения стоимости?
- **Цена** архивации укладывается в ваш бюджет?

Общие решения архивации

Итак, на план архивации влияют емкость, надежность, расширяемость, скорость и цена. Если вы определите, какие из этих факторов наиболее важны для вашей организации, вы примете подходящее решение. Бот некоторые общие рекомендации.

- Ленточные накопители — самые распространенные устройства архивации. Используют для хранения данных кассеты с магнитной лентой. Лента относительно недорога, но не особенно надежна: она может помяться или растянуться, с течением времени — размагнититься и перестать считываться. Средняя емкость кассет с лентой варьируется от 10 Мб до 2 Гб. По сравнению с другими решениями ленточные накопители довольно медленны. Их сильная сторона — невысокая цена.
- **Накопители на цифровой ленте (digital audio tape, DAT)** быстро вытеснили стандартные ленточные накопители. DAT-накопители используют 4-мм и 8-мм ленты. DAT-накопители и ленты дороже стандартных ленточных накопителей, но работают быстрее и вмещают больше данных. DAT-ленты шириной 4 мм могут записывать со скоростью около 30 Мб/мин. и хранить до 16 Гб данных, а 8-мм DAT-ленты — записывать около 10 Мб/мин. и хранить до 36 Гб (со сжатием).
- Ленточная библиотека с автозагрузкой использует набор лент для создания расширенных архивных томов, покрывающих требования всего предприятия. Ленты набора в процессе архивации или восстановления данных

автоматически меняются. В большинстве таких библиотек применяются 4--12 DAT-лент, но их главный минус — высокая цена.

- Магнитооптические накопители объединяют технологии магнитных лент и оптических лазеров. Они надежнее DAT и основаны на 3,5- и 5,25-дюймовых дисках, похожих на дискеты, но более толстые. Емкость магнитооптического диска — 1–4 Гб.
- Дисковые **библиотеки** похожи на ленточные, но в них применяются магнитооптические диски, а не DAT-кассеты. При архивации и восстановлении такие библиотеки загружают и выгружают диски, хранящиеся внутри. Их основной недостаток — дороговизна.
- **Съемные диски,** например Iomega Jaz, все чаще используются в качестве устройств архивации. Они обладают хорошей скоростью и удобны в работе, но стоят дороже ленточных или DAT-накопителей.
- **Дисковые накопители** обеспечивают наивысшую скорость при архивации и восстановлении файлов. Если при архивации на ленту у вас могут уйти часы, то дисковый накопитель позволяет завершить процесс в несколько минут. Никакой другой накопитель не сможет обойти его по скорости. К недостаткам дисковых накопителей следует отнести относительно высокую цену и низкую расширяемость.

Перед использованием средства архивации надо установить. При установке любых устройств архивации, кроме ленточных и DAT-накопителей, необходимо указать ОС контроллеры и драйверы, используемые накопителями. Подробнее об установке накопителей и драйверов см. главу 2.

Покупка и использование лент

Количество лент зависит от того, сколько данных и как часто вы будете архивировать и сколько дополнительных наборов данных вы собираетесь хранить.

Общепринятый способ использования лент — чередующийся график, по которому по очереди используются два или более набора лент. Идея в том, что вы можете увеличить долговечность лент за счет снижения интенсивности их использования и в то же время сократить количество лент, необходимых для хранения данных.

Один из самых распространенных графиков подразумевает использование 10 лент. При этом ленты делят на два набора (но одной ленте на каждый день недели). Как показано ниже, первый набор используется в первую неделю, второй — на следующей (табл. 14-2). В пятницу по графику проводится полная архивация, с понедельника по четверг — добавочная. Если добавить третий набор лент, то сможете по очереди один из наборов хранить в безопасном месте вне офиса.

Табл. 14-2. Добавочная архивация.

День недели	Набор лент 1	Набор лент 2
Пятница	Полная архивация на ленту 5	Полная архивация на ленту 5
Понедельник	Добавочная архивация на ленту 1	Добавочная архивация на ленту 1
Вторник	Добавочная архивация на ленту 2	Добавочная архивация на ленту 2
Среда	Добавочная архивация на ленту 3	Добавочная архивация на ленту 3
Четверг	Добавочная архивация на ленту 4	Добавочная архивация на ленту 4

Совет График с использованием 10 лент разработан для 5-дневной рабочей недели. Если ваша организация работает 7 дней в неделю, необходимо иметь ленты для архивации по субботам и воскресеньям. В этом случае используйте 14 лент: 2 набора по 7. По воскресеньям проводите полную архивацию, а с понедельника по субботу — добавочную.

Архивация данных

В Windows 2000 есть программа Backup (Архивация) для создания архивов данных на локальных или удаленных системах. Вы можете использовать ее для архивирования файлов и панок, восстановления заархивированных файлов и папок, доступа к накопителям, выделенным для Backup, доступа к удаленным ресурсам из окна My Network Places (Мое сетевое окружение), создания образа состояния системы для последующей архивации и восстановления, планирования архивации через Task Scheduler (Планировщик задач) и создания аварийного диска.

Запуск утилиты Backup

Backup можно запустить несколькими способами.

- В консоли Computer Management (Управление компьютером) раскройте System Tools (Служебные программы) и в дереве консоли щелкните System Information (Сведения о системе). Меню обновится и будет включать пункт Tools (Сервис). Щелкните Tools, выберите Windows, а затем — Backup (Архивация).
- В меню Stare (Пуск) выберите Run (Выполнить). В диалоговом окне наберите **ntbackup** и щелкните OK.
- Раскройте меню Start\Programs\Accessories\System Tools (Пуск\Программы\Стандартные\Служебные), а затем — Backup (Архивация данных).

Ниже показано главное окно утилиты Backup (рис. 14-1) с четырьмя вкладками:

- **Welcome** (Добро пожаловать!) содержит приветствие Backup и кнопки для запуска Backup Wizard (Мастер архивации), Restore Wizard (Мастер восстановления) и утилиты Emergency Repair Disk (Диск аварийного восстановления);
- **Backup** (Архивация) предоставляет интерфейс для выбора архивируемых данных; вы можете сохранить данные на локальных или сетевых дисках;
- Restore (Восстановление) предоставляет интерфейс для восстановления заархивированных данных; вы можете восстановить данные в прежнее место или в любое другое место в сети;
- Schedule Jobs (Запланированные задания) позволяет спланировать задания на архивацию по месяцам; вы можете видеть как выполненные задания, так и будущие.

Вы должны иметь необходимые права и полномочия для выполнения архивации и восстановления данных. Члены групп Administrators (Администраторы) и Backup Operators (Операторы архива) могут архивировать и восстанавливать файлы любого типа независимо от того, кто владелец файла и какие разрешений назначены файлу. Кроме того, файл могут архивировать его владельцы и те, кто имеет для него разрешения Read (Чтение), Read and Execute (Чтение и выполнение), Modify (Изменить) или Full Control (Полный доступ).

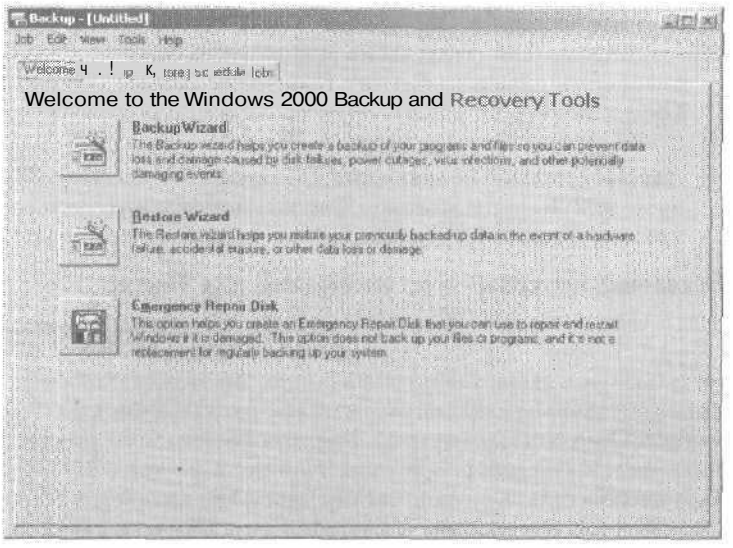


Рис. 14-1. Утилита Windows 2000 Backup предоставляет дружественный интерфейс для архивации и восстановления данных.

Примечание Локальные учетные записи могут работать только с локальной системой, а доменные имеют более высокие полномочия. Поэтому члены локальной группы администраторов могут работать только с файлами на локальной системе, а члены группы администраторов домена вправе работать с файлами во всем домене.

Backup предоставляет расширения для работы с особыми типами данных, перечисленными ниже.

- **Данные состояния системы** включают основные системные файлы, необходимые для восстановления локальной системы. На всех компьютерах есть данные состояния системы, которые нужно сохранить с другими файлами для дальнейшего восстановления ее работоспособности.
- **Данные Exchange Server** включают файлы данных и хранилища информации Exchange. Вам нужно сохранить эти данные для восстановления работы Exchange Server. Этот тип данных доступен только на системах с Exchange Server.

- **Данные съемных ЗУ** хранятся в %SystemRoot%\System32\Ntmsdata. Если вы их архивируете, задайте дополнительный параметр Restore Removable Storage Database (Восстановить базу данных съемных ЗУ) для восстановления конфигурации съемных ЗУ.
- **Данные удаленных хранилищ** хранятся в % SystemRoot%\System32\Remote-storage. **Для восстановления данных** удаленного **хранилища** скопируйте данные **в этот** каталог.

Установка параметров по умолчанию для Backup

Для создания архивов служат вкладка Backup и мастер Backup Wizard. В обоих случаях при архивации данных будут использованы параметры по умолчанию. Вы можете просмотреть или изменить параметры, щелкнув Tools (Сервис), а затем выбрав Options (Параметры). Утилита Backup представляет пять видов параметров по умолчанию: General (Общие), Restore (Восстановление), Backup Type (Тип архива), Backup Log (Журнал архивации) и Exclude Files (Исключение файлов) (рис. 14-2).

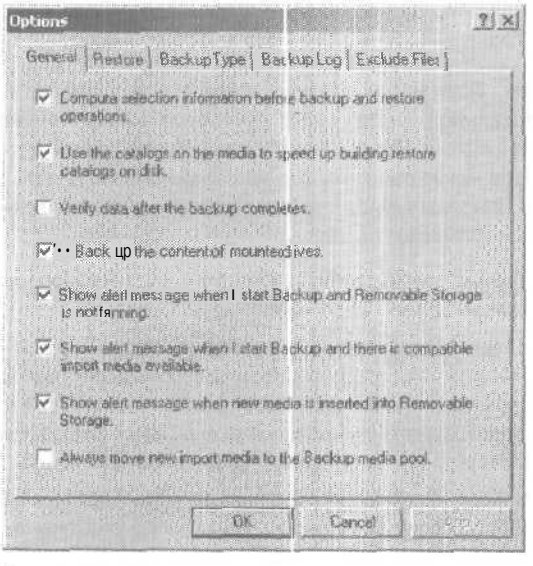


Рис. 14-2. Установка параметров по умолчанию утилиты Backup.

Общие параметры архивации

Общие параметры на вкладке **General окна Options задают** поведение **Backup.**

Табл. 14-3. Общие параметры архивации.

Параметр	Описание
Compute Selection Information Before Backup And Restore Operations (Оценивать информацию о выборе файлов перед выполнением операций архивации или восстановления)	Подсчет числа файлов и байт, которые будут заархивированы или восстановлены в ходе текущего задания архивации или восстановления. Эти сведения будут подсчитаны и выведены перед началом процесса архивации или восстановления.
Use The Catalogs On The Media To Speed Up Building Restore Catalogs On Disk (*Использовать* каталоги носителей для ускорения построения каталогов восстановления на диске)	Выбор каталога носителя для создания на диске каталога, в котором восстанавливаются данные. Это самый быстрый способ построения каталога на диске. Сбросьте этот параметр, если каталога нет, или поврежден, или недоступен по иным причинам.
Verify Data After The Backup Completes (Проверять данные после завершения архивации)	Проверка соответствия архивных данных и исходных данных на жестком диске. Если эти данные не будут совпадать, значит, носитель или файл архива содержит ошибки. В этом случае повторите архивацию, используя другой носитель или файл.
Back Up The Contents Of Mounted Drives (Архивировать содержимое подключенных дисков)	Архивация данных на *подключенном* диске. Если этот флажок установлен, при архивации подключенного диска будет выполнена архивация хранящихся на нем данных. Если флажок не установлен, при архивации подключенного диска будет выполнена архивация только сведений о его путях.
Show Alert Message When I Start Backup And Removable Storage Is Not Running (Выводить предупреждение, если служба съемных носителей не активна при запуске архивации)	Отображение диалогового окна, если при запуске архивации не работает служба съемных носителей. При архивации данных в файл, который затем будет записан на дискету, жесткий или съемный диск, не устанавливайте этот флажок. Если предполагается архивация данных на ленту или другой носитель, управляемый службой съемных носителей, его следует установить.

Табл. 14-3. *(продолжение)*

Параметр	Описание
Show Alert Message When I Start Backup And There Is Compatible Import Media Available (Выводить предупреждение, если при запуске архивации имеется совместимый импортируемый носитель)	Отображение диалогового окна, если при запуске архивации в пуле импортированных носителей доступен новый носитель. При архивации данных в файл, который затем будет записан на дискету, жесткий или съемный диск, не устанавливайте этот флажок. Если предполагается архивация данных на ленту или другой носитель, управляемый службой съемных носителей, его надо установить.
Show Alert Message When New Media Is Inserted Into Removable Storage (Выводить предупреждение, когда новый носитель вставляется в хранилище съемных носителей)	Отображение диалогового окна при обнаружении нового носителя службой съемных носителей. При архивации данных в файл, который затем будет записан на дискету, жесткий или съемный диск, не устанавливайте этот флажок. Если предполагается архивация данных на ленту или другой носитель, управляемый службой съемных носителей, его надо установить.
Always Move New Import Media To Backup Pools (Всегда перемещать новый импортированный носитель в пулы носителей архивации)	Автоматическое перемещение нового носителя, обнаруженного службой съемных носителей, в пул архивации, При архивации данных в файл, который затем будет записан на дискету, жесткий или съемный диск, не устанавливайте этот флажок. Если носители управляются службой съемных носителей и требуется, чтобы все новые носители были доступны только для программы архивации, установите этот флажок.

Установка параметров восстановления и архивации

На поведение процессов архивации и восстановления влияют следующие параметры (табл. 14-4).

Табл. 14-4. Параметры восстановления, типа **архива** и журнала архивации.

Вкладка	Параметр	Описание
Restore (Восстановление)	Do Nor Replace The Files On My Computer * (Recommended)	Включение копирования из архива файлов, копии которых уже имеются на диске. Если

Табл. 14-4. *(продолжение)*

Вкладка	Параметр	Описание
	[Не заменять файл на компьютере (рекомендуется)]	выбран этот параметр, файл восстанавливается, только если его нет на диске. Это самый безопасный режим восстановления.
	Replace The File On Disk If the File On Disk Is Older (Заменять файл на компьютере если только он старее)	Включение замены старых файлов на диске новыми копиями из архива. Если выбран этот параметр, восстанавливаются также файлы, которых нет на диске. Выбор этого параметра может привести к замене некоторых или всех файлов на лиске.
	Always Replace The File On My Computer (Всегда заменять файл на компьютере)	Включение замены всех файлов на диске независимо от того, какие файлы более ранней версии. Если выбран этот параметр, восстанавливаются также файлы, которых нет на диске. Это может привести к потере данных, если в архиве имеются файлы, часто изменяемые на компьютере.
Backup Type (Тип архива)	Default Backup Type (Используемый по умолчанию тип архива)	Список типов архивации. Выберите один из следующих типов: обычный, копирующий, разностный, добавочный и ежедневный.
Backup Log (Журнал архивации)	Detailed (Подробная)	Сохранение подробной записи о выполняемых заданиях архивации и восстановления. Это самый подробный файл журнала, создаваемый программой архивации.
	Summary (Краткая сводка)	Сохранение краткой сводки выполняемых заданий архивации и восстановления. Это самый краткий файл журнала, создаваемый программой архивации.
	None (Никакой)	Отключение создания файла журнала заданий архивации и восстановления.

Просмотр и установка исключений файлов

Многие типы системных файлов по умолчанию исключены из архивации. Вы можете управлять исключениями в окне Options, доступном из меню Tools утилиты Backup.

Просмотр исключений — в оснастке Backup вы можете просмотреть исключения, щелкнув вкладку Exclude Files диалогового окна Options. Исключение файлов основано на владении файлом можно установить как для всех пользователей, так и пользователя, зарегистрировавшегося в системе (рис. 14-3).

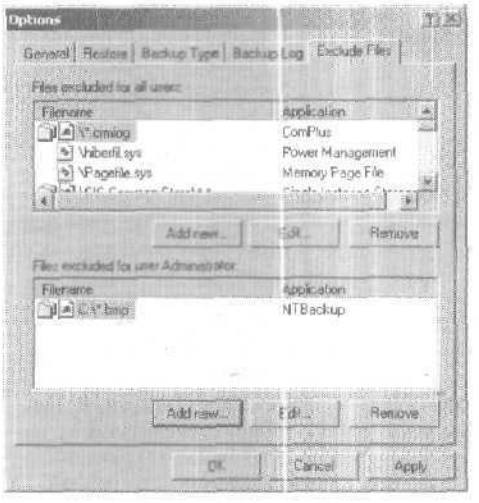


Рис. 14-3. Просмотр существующего исключения файлов для пользователей.

Создание исключений - чтобы исключить дополнительные файлы, сделайте так.

1. В диалоговом окне Options перейдите на вкладку Exclude Files.
2. Если вы хотите исключить файлы, принадлежащие всем пользователям, щелкните Add New (Добавить...) под списком Files Excluded For All Users (Файлы, исключенные для всех пользователей). Появится диалоговое окно Add Excluded Files (Добавление исключаемых файлов) (рис. 14-4).

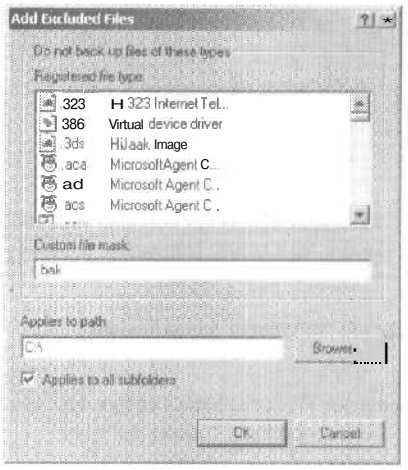


Рис. 14-4. Установка исключений файлов для пользователей.

3. Если вы хотите исключить файлы, владельцем которых являетесь только вы, щелкните Add New (Добавить...) под списком Files Excluded For User Administrator (Файлы, исключенные для пользователя Administrator). Появится диалоговое окно Add Excluded Files (Добавление исключаемых файлов).
4. Вы можете исключить файлы зарегистрированного типа, щелкнув тип файла в списке Registered File Type (Зарегистрированный тип файла). Вы можете исключить пользовательский тип файла, набрав точку и расширение файла в поле Custom File Mask (Особая маска файла). Например, вы можете выбрать .DOC или пользовательский тип .WBK.
5. Введите диск или путь файла в поле Applies To Path (Применяется к пути). Все файлы из всех подкаталогов данного пути будут исключены из архивации, пока вы не сбросите флажок Applies To All Subfolders (применять ко всем подпапкам). Так, если вы ввели C;\ и выбрали Applies To All Subfoiders, все файлы, оканчивающиеся выбранным расширением, будут исключены, где бы они ни встретились на диске C. Щелкните OK.

Изменение исключений — чтобы изменить существующие исключения, сделайте так.

1. В диалоговом окне Options выберите вкладку Exclude Files.
2. Выберите существующее исключение и щелкните Edit (Изменить). Теперь вы можете редактировать исключение файлов.
3. Выберите существующее исключение и щелкните Remove (Удалить). Исключение будет удалено. Щелкните Apply (Припять) по завершении редактирования.

Архивация данных с помощью мастера архивации

Мастер запускается так.

1. Запустите Backup. На вкладке Welcome щелкните Backup Wizard (Мастер архивации), а затем — Next (Далее).

Примечание Вы можете выбрать файлы на вкладке Backup, а затем запустить Backup Wizard. Тогда вы заархивируете только выделенные файлы. Щелкнув Yes (Да), вы сразу перейдете в диалоговое окно, щелкнув No — снимете выделение с выбранных файлов и запустите мастер в обычном режиме.

2. Выберите, что вы хотите архивировать:
   - **Back** Up Everything **On** My **Computer** (Архивировать все данные на этом компьютере) — архивируются все данные на компьютере, включая данные состояния системы;
   - **Back Up Selected Files, Drives, Or Network Data** (Архивировать выбранные файлы, диски или сетевые данные) — архивируются только выбранные данные;
   - **Only Back Up The** System **State Data** (Архивировать только данные состояния системы) — создается архив данных состояния системы.

Примечание Для компьютеров с Windows 2000 Professional и серверов, не являющихся контроллерами доменов, данные состояния системы включают основные загрузочные и системные файлы, реестр Windows и БД COM+. Для контроллеров домена данные состояния системы также включают данные службы каталогов Active Directory и файлы из системного тома fSysvol).

3. Щелкните Next. Если вы хотите выбрать данные для архивации, отметьте желаемые элементы.
   - Сделайте выбор, отметив или сбросив флажки рядом с дисками/папками. Если отметить флажок диска, выбираются все панки и файлы на диске, при сбросе — все папки и файлы на нем исключаются из архивации.
   - Если вы хотите выделить определенный файл или папку, щелкните значок (+). Теперь вы можете выбрать или сбросить флажок отдельного файла/папки. При этом флажок диска затенен, т. е. не все файлы на нем выбраны для архивации.
4. Щелкните Next и выберите тип носителя архива. Выберите имя файла, если хотите сохранить архив в файл. Выберите устройство хранения, если хотите сохранить архив файлов и папок на ленте или съемном диске.

Совет При архивации в файл, как правило, файл архива имеет расширение .BKF; вы можете дать другое расширение. Помните, что хранилище съемных носителей используется для управления лентами и съемными дисками. Если нет ни одного доступного носителя, укажите поиск носителя в пуле. См. раздел «Управление пулом носителей».

5. В ноле Backup Media Or File Name (Носитель архива или имя файла) выберите файл архива или носитель. Если вы архивируете в файл, наберите путь и имя файла или щелкните Browse (Обзор) для его поиска. Если вы архивируете на ленту или съемный диск, выберите ленту или диск для использования.
6. Щелкните Next. Щелкните Advanced (Дополнительно), если хотите изменить параметры по умолчанию или задать расписание для выполнения архивации. Далее следуйте пп. 7–12. Иначе перейдите к п. 13.
7. Выберите тип архивации: обычный, копирующий, разностный, добавочный или ежедневный.
8. Для сохранения данных, предназначенных для внешнего хранилища, выберите Backup Migrated Remote Storage Data (Архивировать данные из внешних хранилищ). При этом архивируются файлы внешнего хранилища. Это позволит вам восстановить файловую систему с необходимой ссылочной целостностью внешнего хранилища.

9. Теперь можно задать параметры проверки и сжатия.
   - **Verify Data After Backup** (Проверить данные после архивации) заставляет Backup проверять данные по завершении архивации. Если этот параметр включен, каждый файл архива сравнивается с оригинальным файлом. Проверка данных защищает архив от ошибок записи и сбоев.
   - **Use Hardware Compression, If Available** (Использовать аппаратное сжатие, если возможно) позволяет Backup сжимать данные при записи на устройство архивации. Этот параметр доступен, только когда устройство поддерживает аппаратное сжатие. Только совместимые устройства смогут прочитать сжатую информацию. Это значит, что данные можно будет восстановить только с накопителя того же изготовителя.
10. Включите параметр копирования данных на выбранный файл, ленту или съемный диск. Чтобы добавить архив к существующим данным, выберите Append This Backup To The Media (Дописать этот архив к данным носителя). Для перезаписи существующих данных выберите Replace The Data On The Media With This Backup (Затереть данные носителя этим архивом). Перезаписывая данные, можно указать, что только владелец или администратор будет иметь доступ к этому архивному файлу, выбрав параметр Allow Only The Owner And Administrator Access (Разрешать доступ к данным этого архива и всем дозаписываемым на этот носитель архивам только владельцу или администратору).
11. По желанию наберите метку архива или метку носителя. Первая задается только для текущего архива, вторая задает метку для ленты или съемного диска.

Примечание Метку носителя можно изменить только при записи на чистую ленту или при перезаписи существующих данных.

12. Определите срок выполнения архивации. Выберите Now (Сейчас) для немедленной архивации или Later (Позже) для задания расписания выполнения архивации. Если вы составляете расписание архивации, введите свой пароль, затем введите имя задания и щелкните Set Schedule (Ус-

тановить расписание). После этого составьте расписание (см. главу 4).

13. Щелкните Finish (Готово) для запуска архивации с параметрами архивации по умолчанию. Запуститься процесс архивации. Вы можете отменить архивацию, нажав Cancel (Отмена) в диалоговых окнах Set Information (Информация о выборе) и Backup Progress (Ход архивации).
14. Backup ведет себя по-разному в зависимости от типа и состояния файла. Если файл открыт, утилита попытается архивировать последнюю записанную версию. Если файл заблокирован, он не будет архивирован. Не будут архивированы и файлы из списка исключений.
15. По завершении архивации щелкните Close (Закрыть) для окончания процесса или Report (Отчет) — для просмотра журнала архивации.

Совет Журналы архивации записываются в виде ASCII-файла и хранятся 8 папке %USERPROFILE%\Local Settings\-Microsoft\WindowsNT\NTBackup\Data. Для поиска журнала архивации используйте атрибут время/дата файла журнала. Имя файла журнала архивации записывается в формате backup##.log, имя первого журнала — backup01.log.

Архивация файлов без помощи мастера

Вы можете провести архинацию файлов вручную.

1. Запустив Backup, щелкните вкладку Backup (рис. 14-5).
2. Снимите существующие выделения файлов и дисков, нажав New (Создать) в меню Job (Задание). Затем щелкните Yes (Да) в предупреждении.
3. Выделите данные для архивации.
   - « Сделайте выбор, отметив или сбросив флажки рядом с дисками или папками. Если отметить флажок диска, все папки и файлы на нем будут выбраны, при сбросе флажка все папки и файлы диска исключаются из архивации.
   - • Если хотите выделить определенный файл или папку, щелкните значок (+). Теперь можете выбрать или сбросить флажок отдельного файла или папки. При этом флажок диска затенен, т. е. не все файлы на нем выбраны для архинации.

- Если хотите сохранить данные состояния системы, выберите флажок System State (Состояние системы) ветви My Computer (Мой компьютер). Для машин Windows 2000 Professional и серверов, не являющихся контроллерами доменов, данные состояния системы включают основные загрузочные и системные файлы, реестр Windows и базу данных COM+. Для контроллеров домена данные состояния системы также включают данные службы каталогов Active Directory и файлы, хранящиеся на системном томе.
- Если вы хотите *архивировать* данные сервера Microsoft Exchange, убедитесь, что отмечен значок Microsoft Exchange в ветви My Computer. Введите UNC-имя того сервера Microsoft Exchange, который нужно сохранить, например **\\CorpMail**.

Рис. 14-5. На вкладке Backup настройте архивацию вручную. Затем щелкните Start Backup.

4. В списке Backup Destination (Место назначения архива) можно выбрать ти] носителя архива. Если вы выбрали File (Файл), архивация будет проводиться в файл, если внешнее хранилище — файлы и папки будут сохраняться на ленту или съемный диск.

Совет Обычно при архивации в файл архиву назначается расширение .BKF, но вы вправе задать и другое расширение. Хранилище съемных носителей используется для управления лентами и съемными дисками. Если нет ни одного доступного носителя, укажите поиск носителя в пуле. См, раздел «Управление пулом носителей».

5. В поле Backup Media Or File Name (Носитель архива или имя файла) выберите файл архива или носитель. Если вы архивируете в файл, наберите путь и имя файла или щелкните Browse (Обзор) для поиска файла, если на ленту или съемный диск — выберите ленту или диск.
6. На вкладке Backup щелкните Start Backup (Архивировать). Появится диалоговое окно Backup Job Information (Сведения о задании архивации) со следующими параметрами (рис, 14-6).
   - **Backup Description** (Описание архива) задает метку архива, которая используется только при текущей архивации.

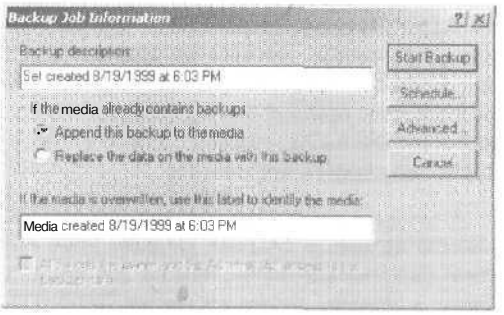


Рис. 14-6. В диалоговом окне Backup Job Information настройте параметры архивации. Затем щелкните Start Backup.

   - **Append This Backup To The Media** (Дозаписать этот архив к данным носителя) добавляет текущее задание архивации к имеющемуся файлу или на имеющуюся ленту. Такая архивация не влияет на данные R файле или на ленте.
   - **Replace The Data On The Media With This Backup** (Затереть данные носителя этим архивом) удаляет файл

архива или все задания архивации, имеющиеся на ленте, перед запуском нового задания архивации.

- If The Media Is Overwritten, Use This Label To Identify The Media (Если носитель перезаписывается, записать метку) задает метку носителя, которая записывается только при использовании чистого носителя или записи поверх существующих данных. Метку носителя можно создать только на новой ленте и при перезаписи имеющейся ленты. Метка носителя не может изменяться на имеющейся ленте, если данные дозаписываются.

7. Щелкните Advanced (Дополнительно...), чтобы изменить параметры по умолчанию.

- Back Up Data That Is In Remote Storage (Архивация данных из внешних хранилищ) — архивация данных, предназначенных для внешних хранилищ. Гарантирует восстановление всей файловой системы, сохраняя нетронутыми необходимые ссылки на внешнее хранилище.
- Verify Data After Backup (Проверить данные после архивации) — сравнение данных из архива и исходных данных, Если этот параметр задан, каждый файл архива сравнивается с оригинальным файлом. Проверка данных защищает архив от ошибок записи и сбоев, но может заметно замедлить архивацию.

Внимание! Архивация системных файлов может заметно увеличить размер архива. В системе Windows 2000 Professional он может увеличиться более, чем на 200 Мб. В Windows 2000 Server к размеру архива добавится 700-1 000 Мб.

- **If Possible, Compress Backup Data To Save Space** (Если возможно, сжимать архивируемые данные) — сжатие архивируемых данных позволяет увеличить объем данных, записываемых на одну ленту. Обычно возможность сжатия данных имеется только в накопителях на магнитной ленте. Если этот параметр недоступен, ленточный накопитель не поддерживает сжатие данных. Только совместимые устройства смогут прочитать сжатую информацию. Это значит, что данные можно будет восстановить лишь с накопителя того же изготовителя.

- Automatically Back Up System Protected Files With The System State (Автоматически архивировать защищенные системные файлы вместе с состоянием системы) — добавление всех системных файлов из системного корневого каталога %SystemRoot% в архив вместе с загрузочными файлами, включаемыми в данные о состоянии системы.
- **Backup Type** (Тип архива) отображает тип архива: обычный, копирующий, разностный, добавочный или ежедневный.

8. Щелкните Schedule (Расписание...) для составления расписания дальнейшей архивации. Когда появится предложение записать текущие параметры архивации, щелкните Yes (Да). Затем наберите имя сценария выбора, а затем щелкните Save (Записать). В окне Scheduled Job Options (Параметры запланированного задания) наберите имя задания, щелкните Properties (Свойства), затем составьте расписание как описано к главе 4. Пропустите оставшиеся пункты.

Примечание Сценарии выбора и журналы архивации сохраняются в папке %USERPROFILE%\Local Settings\Microsoft\WindowsNT\NTBackup\Data. Сценарии выбора сохраняются с расширением .BKS, а журналы архивации — с расширением .LOG. Вы сможете просмотреть содержимое этих файлов в любом стандартном текстовом редакторе.

9. Щелкните Finish для запуска архивации с параметрами архивации по умолчанию. Запустится процесс архивации. Вы можете отменить архивацию, нажав Cancel (Отмена) в диалоговых окнах Set Information (Информация о выборе) и Backup Progress (Ход архивации).
10. Завершив архивацию, щелкните Close (Закрыть) или же Report (Отчет) — для просмотра журнала архивации.

Восстановление данных с помощью мастера

Вы можете восстановить данные с помощью утилиты Windows 2000 Backup, используя Restore Wizard (Мастер восстановления) или вкладку Restore (Восстановление). Чтобы восстановить данные через Restore Wizard, сделайте так.

1. Убедитесь, что необходимый для работы архивный набор загружен в библиотеку.

2. Запустите утилиту Backup. На вкладке Welcome щелкните Restore Wizard (Мастер восстановления), а затем — Next.

Примечание Вы можете выбрать файлы на вкладке Restore и запустить мастер восстановления. При этом будут восстанавливаться только выделенные файлы. Щелкните Yes, чтобы открыть диалоговое окно (рис. 14-8). Щелкнув No, вы снимете выделение с выбранных файлов и запустите мастер в обычном режиме.

3. Вы можете выбрать данные для восстановления (рис. 14-7). В левом части окна отображаются файлы, организованные в тома, в правом — наборы носителей.
   - Отметьте флажки диска, папки или файла, которые хотите восстановить. Если набор носителей, с которым вы будете работать, не отображен, щелкните Import File (Файл импорта) и введите путь к каталогу, где хранится архив.
   - Если вы хотите восстановить данные состояния системы, отметьте флажок System State (Состояние системы). Если вы восстанавливаете файлы на исходное местоположение, текущие данные состояния системы будут заменены на восстанавливаемые. Если восстановление идет па альтернативное местоположение,

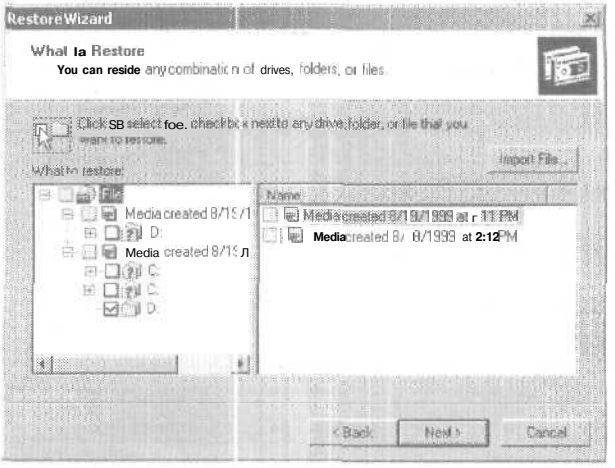


Рис. 14-7. Выбор файлов и папок для восстановления.

будут восстановлены только реестр, системные загрузочные файлы и файлы каталога Sysvol.

Совет По умолчанию Active Directory и другие реплицируемые данные, например данные каталога Sysvol, не восстанавливаются на контроллерах домена. Эта информация восстанавливается только после перезапуска контроллера, что защищает от случайной перезаписи основную информацию домена (см. также раздел «Восстановление Active Directory»).

- Если вы собираетесь восстанавливать Microsoft Exchange, выделите данные Microsoft Exchange. Перед запуском восстановления вы увидите диалоговое окно Restoring Microsoft Exchange (Восстановление Microsoft Exchange). Если вы собираетесь восстанавливать Information Store (Хранилище информации), наберите UNO имя сервера Microsoft Exchange, например **CorpMail**. При восстановлении другого сервера выберите Erase All Existing Data (Уничтожить все существующие данные): все существующие данные уничтожатся, и будет создано новое хранилище.

4. Щелкните Next, затем — Advanced (Дополнительно), чтобы изменить параметры по умолчанию, и выполните пп. 5-7. Или же перейдите к п. 8.
5. Выберите место для восстановления.
   - Original **Location** (Исходное размещение) — файлы и папки восстанавливаются в то место, с которого были заархивированы.
   - **Alternate Location** (Альтернативное размещение) - данные восстанавливаются в указанную папку с сохранением структуры каталогов. Выбрав этот параметр, введите путь к папке или используйте кнопку Browse для поиска нужной папки.
   - Single Folder (Единственная папка) — все файлы восстанавливаются в одну папку без сохранения структуры каталогов. Выбрав этот параметр, введите путь к папке или используйте кнопку Browse для поиска нужной папки.

Совет Если вы не уверены в необходимости восстанавливать данные в исходное размещение, выберите Alternate Path и задайте новое расположение, например C:\temp. По-

скольку файлы находятся во временной папке, их можно сравнить с существующими файлами и решить, восстанавливать ли их. Помните: вам нужно всегда восстанавливать данные, архивированные с дисков с файловой системой NTFS на диски NTFS. Только тогда можно быть уверенным, что восстановятся разрешения и сохранятся шифрование и сжатие NTFS.

6. Задайте способ восстановления файлов.
   - Do Not Replace The Files On **My** Computer (Recommended) [Не заменять имеющийся на диске файл (рекомендуется)] — выберите этот параметр, если не хотите копировать поверх существующих файлов.
   - **Replace** The File **On Disk Only If the File On Disk Is Older** (Заменять файл на диске, только если он старее архивной копии) — выберите этот параметр, чтобы заменить старые файлы на диске более свежими версиями из архива.
   - **Always Replace The File On** My **Computer** (Всегда заменять имеющийся на диске файл) — выберите этот параметр, чтобы заменить все файлы на диске файлами из архива.
7. Вы можете восстановить данные безопасности и специальные системные файлы, задав следующие параметры (если они доступны).
   - **Restore Security** (Восстановление безопасности) - восстанавливаются настройки безопасности для файлов и папок на томах NTFS.
   - **Restore** Removable Storage **Database** (Восстановление базы данных съемных носителей) — восстанавливается конфигурация съемных носителей, если был сохранен каталог %SystemRoot%\System32\Ntmsdata. При установке этого параметра вся существующая информация о съемных носителях будет удалена.
   - **Restore Junction Points, Not The Folder And File** Data They **Reference** (Восстановление точек соединения, а не папок и файлов, на которые они ссылаются) - восстанавливаются ссылки на сетевые диски, но не сами данные, расположенные на этом диске. По сути, вы восстанавливаете папки, ссылающиеся на сетевой накопитель.

8. Щелкните Next, а затем Finish. При необходимости введите путь или имя архива. Вы можете прервать восстановление, щелкнув Cancel в окнах Operation Status (Информация о выборе) и Restore Progress (Ход восстановления).
9. Завершив восстановление, щелкните Close (Закрыть) или же Report (Отчет) — для просмотра журнала, содержащего информацию о ходе процесса восстановления.

Восстановление данных без помощи мастера

Данные можно восстановить вручную.

1. При необходимости загрузите архивный набор из библиотеки.
2. Запустите утилиту Backup и перейдите на вкладку Restore (Восстановление) (рис, 14-8).

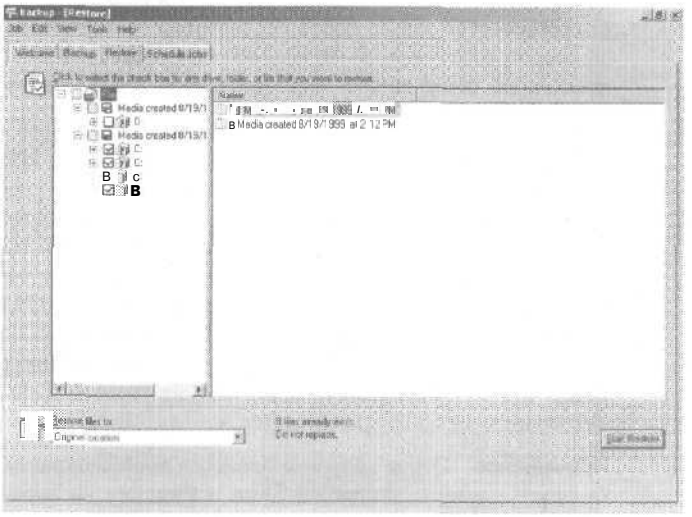


Рис. 14-8. Выбор файлов и папок для восстановления.

3. Выберите данные для восстановления. В левом окне отображаются файлы, организованные в тома. В правом окне показаны наборы носителей.
   - Отметьте флажки диска, панки или файла, которые хотите восстановить. Если набор носителей, с которым вы собирались работать, не отображен, щелкните пра-

вой кнопкой файл в левом окне, выберите Catalog (Каталог), затем наберите имя или путь используемого каталога.

- Если вы хотите восстановить данные состояния системы, отметьте флажок System State (Состояние системы). Если вы восстанавливаете файлы на исходное местоположение, текущие данные состояния системы будут заменены на восстанавливаемые, Если восстановление идет на альтернативное местоположение, будут восстановлены только реестр, системные загрузочные файлы и файлы каталога Sysvol. Вы сможете восстановить данные состояния только на локальной системе.

Совет По умолчанию Active Directory и другие реплицируемые данные, например данные каталога Sysvol, не восстанавливаются на контроллерах домена. Эта информация восстанавливается только после перезапуска контроллера, что защищает от случайной перезаписи основную информацию домена (см. также раздел «Восстановление Active Directory»).

- Если вы собираетесь восстанавливать Microsoft Exchange, выделите данные Microsoft Exchange. Перед запуском восстановления вы увидите диалоговое окно Restoring Microsoft Exchange (Восстановление Microsoft Exchange). Если вы собираетесь восстанавливать Information Store (Хранилище информации), наберите UNC-имя сервера Microsoft Exchange, например **CorpMail**. При восстановлении другого сервера выберите Erase All Existing Data (Уничтожить все существующие данные): все существующие данные уничтожатся, и будет создано новое хранилище.

Примечание Перед запуском процесса восстановления остановите службы Information Store и Directory на сервере. После восстановления перезапустите их.

4. В списке Restore Files To (Восстановить файлы в) выберите место для восстановления.
   - Original Location (Исходное размещение) — файлы и папки восстанавливаются па то место, с которого они были архивированы.

- **Alternate Location** (Альтернативное размещение) - данные восстанавливаются в указанную папку с сохранением структуры каталогов. Выбрав этот параметр, введите путь к папке или используйте кнопку Browse для поиска нужной папки.
- Single **Folder** (Единственная папка) — все файлы восстанавливаются в одну папку без сохранения структуры каталогов. Выбрав этот параметр, введите путь к папке или используйте кнопку Browse для поиска нужной папки.

5. Задайте способ восстановления файлов. Щелкните Tools (Сервис), а затем Options (Параметры). Появится диалоговое окно Options. Доступны следующие способы:
   - **Do Not Replace The** Files On My Computer **(Recommended)** [Не заменять имеющийся на диске файл (рекомендуется)] — выберите этот параметр, если вы не хотите копировать поверх существующих файлов;
   - **Replace** The File **On Disk Only** If the File **On Disk Is Older** (Заменять файл на диске только если он старее архивной копии) — выберите этот параметр, чтобы заменить старые файлы на диске более свежими версиями из архива;
   - **Always Replace** The File **On** My **Computer** (Всегда заменять имеющийся на диске файл) — выберите этот параметр, чтобы заменить все файлы на диске файлами из архива.
6. На вкладке Restore щелкните Start Restore (Восстановить). Появится диалоговое окно Confirm Restore (Подтверждение восстановления).
7. Если вы хотите задать дополнительные параметры восстановления, щелкните Advanced (Дополнительно) и установите такие параметры.
   - **Restore Security** (Восстановление безопасности) - восстановление параметров безопасности для восстанавливаемых файлов и папок. В параметры безопасности входят разрешения па доступ, записи аудита и сведения о владельце. Этот флажок доступен, только если архивация данных проводилась с тома NTFS Windows 2000 и восстановление проводится также на том NTFS Windows 2000.

- **Restore Removable Storage Database** (Восстановление базы данных съемных носителей) — восстаовление базы данных съемных носителей, расположенной в папке %SystemRoot%\System32\Ntmsdata. База данных съемных носителей автоматически архивируется при каждой архивации системного корневого каталога. Если для управления носителями не используются съемные носители, включать этот параметр не надо.
- **Restore Junction Points, And Restore** File **And Folder Data Under Junction** Points **To The Original Location** (Восстановление точек соединения, а также ссылок для файлов и папок ниже соединения на исходное размещение) — восстановление точек соединения на жестком диске, а также данных, на которые указывают эти точки соединения. Если этот флажок не помечен, точки соединения будут восстановлены, но данные, на которые они указывают, будут недоступны.
- **When Restoring Replicated Data Sets, Mark The Restored Data As The Primary Data For All Replicas (При** восстановлении реплицируемых наборов данных помечать восстановленные данные как основные для всех реплик) — если этот флажок установлен, восстановленные данные службы репликации файлов будут реплицированы на серверы-подписчики. При восстановлении данных FRS этот флажок должен быть помечен. Если не помечен, восстанавливаемые данные FRS не смогут быть реплицированы на другие серверы, так как восстановленные данные будут старше текущих на других серверах. Это повлечет замену другими серверами восстановленных данных; таким образом, восстановление данных FRS будет предотвращено.
- **Preserve** Existing Volume **Mount Points** (Сохранить существующие точки подключения томов) — если этот флажок установлен, в ходе восстановления не будет выполняться замена точек подключения томов, имеющихся в разделе или на томе, на который выполняется восстановление. Обычно его следует помечать при восстановлении данных на целом диске, в томе или разделе. При этом сохраняются текущие размещения томов.

8. В диалоговом окне Confirm Restore щелкните OK для запуска процесса восстановления. При необходимости введите путь или имя архива. Вы можете прервать восстановление, щелкнув Cancel в диалоговых окнах Operation Status (Информация о выборе) и Restore Progress (Ход восстановления).
9. Завершив восстановление, щелкните Close (Закрыть) или же Report (Отчет) для просмотра журнала, содержащего информацию о ходе процесса восстановления.

Восстановление Active Directory

Сначала надо определить, в каком режиме восстанавливать данные состояния контроллера: полномочном или неполномочном. По умолчанию выбран последний. В этом режиме Active Directory и другие реплицируемые данные восстанавливаются с использованием информации с других контроллеров. Поэтому вы можете безопасно восстановить отказавший контроллер без потери новой информации Active Directory. С другой стороны, если вы пытаетесь восстановить Active Directory во всей сети с использованием архивных данных, вы должны провести полномочное восстановление. В этом режиме данные восстанавливаются на одном контроллере домена, а затем реплицируются на другие.

Чтобы восстановить Active Directory на контроллере домена с дальнейшей репликацией восстановленных данных но всей сети, сделайте так.

1. Выключите сервер контроллера домена.
2. Запустите сервер. В процессе загрузки на этапе выбора ОС нажмите F8 для входа в безопасный режим.
3. Выберите Directory Services Restore Mode (Режим восстановления служб каталогов).
4. После запуска системы восстановите данные состояния системы и другие необходимые файлы с помощью утилиты Backup.
5. После восстановления данных, но перед перезапуском системы с помощью инструмента Ntdsutil пометьте объекты как полномочные. Проверьте данные Active Directory.
6. Перезапустите сервер. После загрузки сервера данные Active Directory должны реплицироваться по домену.

Архивация и восстановление данных удаленной системы

Утилита Windows 2000 Backup позволяет архивировать данные удаленных систем. Для этого перед началом архивации нужно создать сетевые диски удаленных файловых систем. При архивации данных с сетевых дисков убедитесь, что выбран параметр Back Up The Contents Of Mounted Drives (Архивировать содержимое подключенных дисков). Иначе будут сохранены только ссылки на папки, но не сами данные.

Утилита Backup позволяет восстановить данные удаленных систем. При этом вы можете указать место восстановления в окне My Network Places (Мое сетевое окружение). Если вы восстанавливаете данные на сетевой диск взамен существующей системы, убедитесь, что отмечен флажок Restore Junction Points, And Restore File And Folder Data Under Junction Points To The Original Location (Восстановление точек соединения, а также ссылок для файлов и папок ниже соединения на исходное размещение).

Подготовка и аварийное восстановление

Архивация — это только часть общего плана аварийного восстановления. Для полной уверенности в возможности восстановить систему в любой ситуации вам понадобятся диски аварийного восстановления и загрузочные диски. Возможно, понадобится установить Recovery Console (Консоль восстановления).

Чтобы восстановить систему, сделайте так.

1. Попытайтесь запустить систему в безопасном режиме (см. раздел «Запуск системы в безопасном режиме»).
2. Попытайтесь восстановить систему с помощью диска аварийного восстановления (если он есть) (см. раздел «Использование диска аварийного восстановления»).
3. Попытайтесь восстановить систему из Recovery Console (см. раздел «Работа с Recovery Console»).
4. Восстановите систему из архива. Убедитесь, что были восстановлены данные состояния системы и необходимые файлы.

Создание диска аварийного восстановления

Диск аварийного восстановления поможет восстановить систему, если она не загружается. На этом диске хранятся основные системные файлы, загрузочный сектор и окружение для запуска системы. Вам следует создать такие диски для каждого компьютера сети, начиная с серверов Windows 2000. Кроме того, их нужно обновлять при установке служебных пакетов, работе с загрузочным диском или модификации окружения загрузки.

Совет По завершении установки ОС основная информация для восстановления будет записана в папку %SystemRoot%\Repair системного раздела. В папке Repair хранится копия данных локального диспетчера учетных записей безопасности (Security Account Manager, SAM) и других системных файлов. Но папка не содержит архива реестра Windows. При создании аварийного диска восстановления вам следует заархивировать реестр.

Диск аварийного восстановления создается так.

1. Запустите утилиту Backup. На вкладке Welcome щелкните Emergency Repair Disk (Диск аварийного восстановления).
2. Когда вас попросят, вставьте чистую отформатированную дискету в дисковод.
3. Чтобы заархивировать реестр, пометьте флажок Also Backup The Registry To The Repair Directory (Архивировать реестр в папку восстановления). Архив реестра будет создан в папке %SystemRoot%\Repair. Для восстановления реестра необходимо использовать Recovery Console,
4. Щелкните OK. По окончании процесса выньте дискету и пометьте ее как диск аварийного восстановления системы.

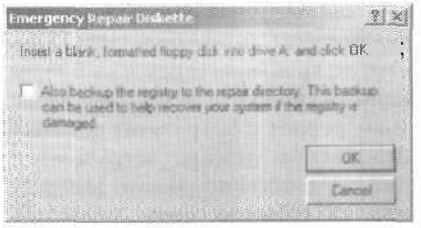


Рис. 14-9. Вставьте чистую дискету в ответ на запрос. Вы также можете сохранить реестр.

Создание загрузочных дисков

Вам нужно создать загрузочные диски для всех версий Windows 2000, работающих в сети. Например, если в сети работают ОС Windows 2000 Professional и Windows 2000 Server, загрузочные диски надо создать для обеих версий, Загрузочные диски позволяют запустить систему, а затем с помощью диска аварийного восстановления и Recovery Console — восстановить ее работоспособность.

Примечание Если ваши компьютеры поддерживают загрузку с CD-ROM, загрузочные диски создавать не нужно. Просто при запуске системы вставьте установочный диск Windows 2000 в CD-ROM.

Загрузочные диски создаются так.

1. Вставьте компакт-диск Windows 2000 в привод CD-ROM.
2. Щелкните Start (Пуск), а затем Run (Выполнить).
3. В диалоговом окне Run наберите **h:\bootdisk\makeboot a:**, где *h* — буква CD-ROM, *a* — буква дисковода. Щелкните OK.
4. Вам понадобится четыре чистых дискеты. Вставьте чистую отформатированную дискету в дисковод и нажмите любую клавишу.
5. Когда закончится запись, выньте дискету и проставьте на ней порядковый номер. Повторите процедуру для оставшихся дискет.

Запуск системы в безопасном режиме

Если система не загружается в обычном режиме, вы можете использовать безопасный режим для восстановления работоспособности и поиска неисправностей. В этом режиме загружаются только основные файлы, службы и драйверы, включая драйверы мыши, клавиатуры, монитора, хранилищ данных и видеоадаптера. Сетевые драйверы и службы в этом режиме не запускаются, пока вы не выберете пункт Safe Mode With Networking (Безопасный режим с загрузкой сетевых драйверов). Поскольку в безопасном режиме загружается ограниченный набор информации о конфигурации, это способно помочь выявить неполадки. Обычно можно обойтись безопасным режимом загрузки, не применяя диск аварийного восстановления или Recovery Console.

В безопасном режиме система запускается так.

1. Запустите (перезапустите) систему.
2. Б процессе загрузки на этапе выбора ОС нажмите F8.
3. Используя стрелки, выберите безопасный режим и нажмите Enter. Выбор безопасного режима зависит от ситуации. Вот основные варианты загрузки.
   - **Safe Mode** (Безопасный режим) — в процессе инициализации загружаются только основные файлы, службы и драйвера. Загружаются драйверы мыши, клавиатуры, монитора, хранилищ данных и видеокарты. Ни одна сетевая служба или драйвер не запускаются.
   - **Safe Mode With Command Prompt** (Безопасный режим с поддержкой командной строки) — загружаются основные файлы, службы и драйверы. Затем вместо графического интерфейса Windows 2000 запускается командная строка. Ни одна сетевая служба или драйвер не запускаются.
   - Safe **Mode** With **Networking** (Безопасный режим с загрузкой сетевых драйверов) — загружаются основные файлы, службы и драйверы, а также службы и драйверы, необходимые для работы с сетью.
   - **Enable Boot Logging** (Включить протоколирование загрузки) — в журнале загрузки создаются записи всех событий запуска.
   - Enable **VGA Mode** (Включить режим VGA) — система загружается в режиме VGA. Это полезно, когда настройки дисплея не поддерживаются монитором.
   - **Last Known Good** Configuration (Загрузка последней удачной конфигурации) — запуск компьютера в безопасном режиме с использованием информации из реестра, сохраненной после последнего завершения работы.
   - **Directory Services Recovery Mode** (Восстановление службы каталогов) — запуск системы в безопасном режиме и восстановление службы каталогов. Доступно только на контроллерах домена Windows 2000.
   - **Debugging Mode** (Режим отладки) — запуск системы в режиме отладки ошибок ОС.

4. Если проблема не проявилась при запуске в безопасном режиме, вы можете исключить параметры по умолчанию и драйверы основных устройств из списка возможных причин проблемы. Если проблемы возникают при добавлении нового устройства или обновлении драйвера, используйте безопасный режим загрузки для удаления устройства и отмены обновления драйвера.

Восстановление системы с помощью диска аварийного восстановления

Если вы не можете запустить и восстановить работоспособность системы в безопасном режиме, ваш следующий шаг - применение диска аварийного восстановления. Его используют в двух ситуациях. Первая: повреждение загрузочного раздела и основных системных файлов. Вторая: проблема в настройке параметров загрузки. Однако вы не сможете восстановить реестр. Для этого понадобится Recovery Console. С помощью диска аварийного восстановления систему восстанавливают так.

1. Вставьте компакт-диск Windows 2000 или другой загрузочный диск и перезапустите компьютер. При загрузке с дискет по мере необходимости вставляйте дополнительные загрузочные дискеты.
2. Когда запуститься программа установки, следуйте указаниям, а затем выберите Repair (Восстановление), нажав клавишу R.
3. Вставьте компакт диск Windows 2000 в привод CD-ROM, если вы этого не сделали.
4. Выберите аварийное восстановление, нажав R, а затем нажмите клавишу:
   - M — для ручного восстановления, чтобы восстановить системные файлы, загрузочный раздел или параметры загрузки; только опытным пользователям и администраторам следует использовать этот режим;
   - F — для быстрого восстановления, чтобы система Windows 2000 сама попыталась решить проблемы с системными файлами, загрузочным разделом и параметрами загрузки.

5. Вставьте диск аварийного восстановления. Поврежденные или отсутствующие файлы будут переписаны с компакт-диска Windows 2000 или из папки %SystemRoot%\Repair системного раздела. Возможно, после записи файлов придется переустановить пакеты обновлений и провести другие изменения.
6. Если восстановление прошло успешно, система перезагрузится в обычном режиме. Иначе вам придется использовать Recovery Console.

Работа с Recovery Console

Recovery Console — одна из последних возможностей восстановить систему. Она работает в режиме командной строки и идеально подходит для решения проблем с файлами, дисками и службами. Recovery Console позволяет выявить и устранить ошибки загрузочного сектора и главной загрузочной записи, подключить и отключить драйверы устройств и службы, изменять атрибуты файлов томов FAT, FAT32 и NTFS; читать и записывать файлы томов FAT, FAT32 и NTFS, копировать файлы с CD-ROM или дисковода на жесткие диски; проверять и форматировать диски.

Вы можете запустить Recovery Console с загрузочного диска или установить ее в качестве варианта загрузки.

Установка Recovery Console в качестве варианта загрузки

На системах с частыми и регулярными сбоями можно установить Recovery Console в качестве одного из вариантов загрузки. Тогда для доступа к Recovery Console не нужны загрузочные диски. Этот вариант работает, только если система загружена. Если вы не в состоянии загрузить систему, см. раздел «Запуск Recovery Console».

В качестве варианта загрузки Recovery Console устанавливается так.

1. Вставьте компакт-диск Windows 2000 в привод CD-ROM,
2. Щелкните Start (Пуск), а затем Run (Выполнить). Появится диалоговое окно Run.
3. Наберите в поле h:\i386\winnt32.exe **/cmdcons**, где *h* – буква вашего CD-ROM.
4. Щелкните OK, а затем Yes (Да). Recovery Console будет установлена как вариант загрузки.

Примечание Обычно только администратор может устанавливать и запускать Recovery Console. Чтобы разрешить обычным пользователям запускать Recovery Console, включите политику Auto Admin Logon на локальном компьютере (из раздела Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options/Auto Admin Logon).

Запуск Recovery Console

Если система не загружается и вы не можете установить Recovery Console в качестве варианта загрузки, компьютер и Recovery Console можно запустить так.

1. Вставьте компакт-диск Windows 2000 или другой загрузочный диск и перезапустите компьютер.
2. Когда запуститься программа установки, следуйте указаниям, а затем выберите Repair (Восстановление), нажав клавишу R.
3. Вставьте компакт диск Windows 2000 в CD-ROM, если вы этого не сделали.
4. Выберите Recovery Console, нажав С. Введите пароль администратора в ответ па соответствующее предложение.
5. После запуска системы вы увидите командную строку, в которой можно набирать команды Recovery Console. Для выхода из консоли и перезагрузки компьютера наберите **exit.**

Команды Recovery Console

Recovery Console работает в режиме командной строки. Ниже перечислены доступные команды (табл. 14-5).

Табл. 14-5. Команды Recovery Console.

Команда	Описание
ATTRIB	Изменение атрибутов файла или каталога
BATCH	Выполнение набора команд **из** текстового файла
CD	Изменение текущего каталога
CHKDSK	Запуск утилиты Chkdsk для проверки целостности диски
CLS	Очистка экрана
COPY	Копирование файла в другое место
DEL	Удаление одного или нескольких файлов

Табл. 14-5. *(продолжение)*

Команда	Описание
DIR	Отображение списка файлов и каталогов
DISABLE	Отключение системной службы или драйвера устройства
DISKPART	Управление разделами на жестких дисках
ENABLE	Отключение или активация системной службы или драйвера устройства
EXIT	Выход из Recovery Console и перезагрузка компьютера
EXPAND	Разуплотнение сжатых файлов
FIXBOOT	Запись нового загрузочного сектора
FIXMBR	Восстановление главной загрузочной записи
FORMAT	Форматирование диска
HELP	Вывод списка команд Recovery Console
LISTSVC	Вывод списка служб и драйверов, доступных на этом компьютере
LOGON	Вход в установленную ОС Windows 2000
MAP	Отображение назначений букв дисков
MD	Создание каталога
MORE	Вывод содержимого текстового файла
REN	Переименование файла
RD	Удаление каталога
SET	Вывод и изменение значений переменных окружения
SYSTEMROOT	Переход в системную папку
TYPE	Вывод содержимого текстового файла

Удаление Recovery Console

Если вам не требуется загружать Recovery Console, се можно удалить.

1. Запустите Windows Explorer (Проводник) и выберите диск, на который вы установили Recovery Console. Обычно это загрузочный диск.
2. В меню Tools (Сервис) выберите Folder Options (Свойства панки).
3. На вкладке View (Вид) выберите Show Hidden Files And Folders (Показывать скрытые файлы и папки) и сбросьте

флажок Hide Protected Operating System Files (Скрывать защищенные системные файлы). Щелкните OK.

4. В правой панели вы увидите корневой каталог загрузочного диска. Удалите нанку Cmdcons и файл Cmldr.
5. Правой кнопкой щелкните файл Boot.ini и выберите Properties (Свойства).
6. В окне свойств сбросьте флажок Read-Only (Только чтение) и щелкните OK..
7. Откройте файл Boot.ini в Notepad (Блокнот). Удалите запись, запускающую Recovery Console. Она выглядит так:

```
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows 2000 Recovery Console" /cmdcons
```

8. Сохраните файл Boot.ini и измените его атрибут на Read-Only.

Recovery Console больш е не будет появляться в списке вариантов загрузки. Позже вы можете переустановить консоль (см. также раздел «Запуск Recovery Console»).

Управление пулом носителей

Наборы лент организованы в пулы носителей, работа с которыми описана ниже.

Понятие пулов носителей

Управлять пулом носителей можно из оснастки Computer Management (Управление компьютером) в поддереве Removable Storage (Съемные ЗУ). Все носители в Removable Storage относятся к определенным типам. Концепция пула носителей очень динамична. Библиотеки могут иметь множество пулов, несколько пулов носителей могут охватывать несколько библиотек.

Можно использовать пульт для организации иерархии, в которой пулы верхнего уровня будут включать пулы нижнего уровня, а эти пулы в свою очередь будут содержать наборы лент или дисков.

В Removable Storage пулы разделены на следующие типы.

- **Unrecognized** (Неопознанные) — пул содержит носители, не определенные Removable Storage, например, новые носители, на которые еще не производилась запись. Что-

бы сделать неопознанные носители доступными для использования, переместите их в пул свободных носителей. Если перед этим вы извлечете носитель, он автоматически удалится из базы данных Removable Storage и не будет больше отображаться.

- **Free** (Свободные) — содержит носители, которые в настоящий момент не используются и не хранят данные. Эти носители доступны приложениям.
- **Import** (Импортированные) — содержит носители, которые были опознаны Removable Storage, но не использовались ранее, в особенности системой Removable Storage. Скажем, если вы переместили носитель из одного места в другое, он может отображаться как импортированный. Для повторного использования носителя на новом месте переместите его в пул свободных носителей или в пул носителей приложений.
- Application (Приложение) — пул содержит носители, используемые и управляемые каким-то приложением, например Windows 2000 Backup. Пулом этого типа могут управлять члены групп Administrators и Backup Operators. Вы можете настроить пул носителей приложений для автоматического переноса носителей из пула свободных носителей. Бы не можете перемещать носители приложений между пулами.

Пулы свободных, неопознанных и импортированных носителей относятся к так называемым пулам системных носителей. В отличие от пула носителей приложения вы не можете удалить пулы системных носителей.

Подготовка носителей для использования в пуле свободных носителей

Если носители содержат никем не используемую информацию, вы можете инициализировать носитель и подготовить его для работы в пуле свободных носителей. При этом вы уничтожите информацию на носителе.

Чтобы подготовить носитель к использованию в пуле, сделайте так.

1. В консоли Computer Management откройте Removable Storage и дважды щелкните Physical Locations (Физическое размещение).

2. Разверните библиотеку и папку носителя библиотеки, дважды щелкнув их.
3. Правой кнопкой щелкните носитель и выберите Prepare.
4. Щелкните Yes.

Перемещение носителя в другой пул

Вы можете переместить носитель в другой пул, сделав его доступным для использования.

1. В оснастке Computer Management откройте Removable Storage и дважды щелкните Physical Locations (Физическое размещение).
2. Разверните библиотеку и папку носителя библиотеки, дважды щелкнув их.
3. Перетащите желаемый носитель из правой панели на пул в дереве консоли.

Внимание! Перемещение носителя в пул свободных носителей уничтожит данные на носителе. Кроме того, нельзя переместить носители, предназначенные только для чтения, в пул свободных носителей.

Создание пулов носителей приложений

1. В Removable Storage правой кнопкой щелкните Media Pools (Пулы носителей) и выберите Create Media Pool (Создать пул носителей). Или щелкните правой кнопкой существующий пул носителей приложений, а затем щелкните Create Media Pool.
2. В диалоговом окне Create New Media Pool Properties (Свойства: Создать новый пул носителей) наберите имя и описание пула носителей.
3. Если пул содержит другие пулы носителей, выберите Contains Other Media Pools (Содержит другие пулы носителей). Иначе щелкните Contains Media Of Type (Содержит носители типа) и выберите соответствующий тип носителя из списка,
4. Завершите процесс, щелкнув OK. Можете назначить носитель и настроить безопасность (см. разделы «Настройка политики выделения и изъятия» и «Настройка разрешений доступа для съемных ЗУ»).

Изменение типа носителей в пуле носителей

Каждый пул может содержать только носители одного типа. Обычно тип носителей задается при создании пула, но вы можете его менять.

1. В Removable Storage дважды щелкните Media Pools.
2. Правой кнопкой щелкните пул, с которым работаете, и выберите Properties.
3. На вкладке General (Общие) щелкните Contains Media Of Type (Содержит носители типа) и выберите соответствующий тип носителя из списка.

Настройка политики выделения и изъятия

Вы можете настроить пулы носителей приложений для автоматического выделения и изъятия свободных носителей. При этом, если приложению понадобится носитель, оно его получит. Если носитель больше не нужен, он будет возвращен в пул свободных носителей.

Носители настраиваются, размещаются и освобождаются так.

1. В Removable Storage **дважды** щелкните Media Pools.
2. Правой кнопкой щелкните пул, с которым работаете, и выберите Properties. Этот пул должен содержать носители определенного типа и не должен быть контейнером для других пулов носителей.
3. Флажки на вкладке General позволяют управлять выделением носителей.
   - **Draw Media From Free Media** Pool (Выбрать носитель из пула свободных носителей) — автоматическое перемещение лент или дисков из пула свободных носителей в данный пул при необходимости. Если этот флажок не помечен, при нехватке носителей ленты или диски придется перемещать из пула свободных носителей вручную.
   - Return **Media To Free Media Pool** (Вернуть носитель в пул свободных носителей) — автоматический возврат лент или дисков в пул свободных носителей, если они больше не требуются приложению. Если этот флажок не помечен, ненужные ленты и диски придется возвращать в пул свободных носителей вручную, чтобы они были доступны другим приложениям.

- Limit Reallocations (Не более) — ограничение числа перераспределений лент и носителей из пула свободных носителей в другие пулы. Если этот флажок помечен, измените значение по умолчанию, введя другое значение.

4. Щелкните OK.

Удаление пулов носителей приложений

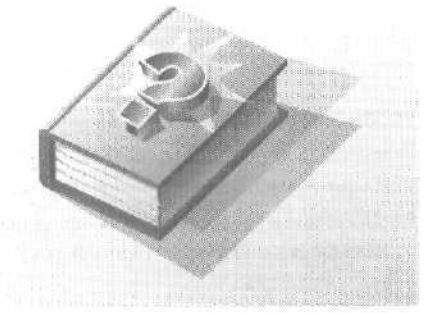
Вы можете удалить пулы носителей приложений, щелкнув правой кнопкой пул и выбрав Delete (Удалить). Удаляйте только ненужные пулы носителей.

Примечание Вы не сможете удалить пулы носителей приложений, созданные Windows 2000, такие как Backup и Remote Storage, — их использует ОС.

Часть IV

Администрирование сети Microsoft Windows 2000

Эта часть посвящена проблемам администрирования сетей Microsoft Windows 2000. Глава 15 содержит сведения по установке, настройке и тестированию сетей TCP/IP. В главе 16 обсуждаются установка и настройка локальных принтеров и сетевых серверов печати и устранение неполадок, связанных с их работой. В главе 17 рассказывается об управлении клиентами и серверами DHCP. В главе 18 рассматривается настройка клиентов и серверов WINS. И, наконец, глава 19 посвящена настройке DNS в сетях Windows 2000.



Глава 15

Управление сетями TCP/IP

Для передачи информации между компьютерами используются базовые сетевые протоколы, встроенные в Microsoft Windows 2000. Мы рассмотрим протокол управления передачей/межсетевой протокол (Transmission Control Protocol/ Internet Protocol, TCP/IP). TCP/IP — это совокупность протоколов и служб, обеспечивающих передачу информации по сети, TCP/IP — основной протокол, используемый в межсетевых коммуникациях. В сравнении с другими сетевыми протоколами настроить TCP/IP довольно сложно, однако в настоящее время он самый универсальный.

Эта глава посвящена настройке и управлению сетями TCP/IP. При организации сети TCP/IP нужно указать, как компьютер будет направлять информацию и обращаться к другим компьютерам. Настроив параметры TCP/IP, нужно сделать компьютер членом сети, чтобы он смог получить доступ к ее ресурсам.

Примечание Права установки и управления сетью TCP/IP определяются **групповой** политикой (см. User Configuration\Network\Network And Dial-Up Connections и Computer Configuration\System\Group Policy) — **см.** о ней **главу 4.**

Установка сети TCP/IP

Для организации сети TCP/IP нужно установить одну или несколько сетевых плат и настроить протокол TCP/IP.

Установка сетевой платы

Сетевая плата — это устройство, предназначенное для обмена данными по сети. Вот как ее установить и настроить.

1. Выключите компьютер из розетки, установите сетевую плату в соответствующий разъем и загрузите систему.

2. При загрузке Windows 2000 должна автоматически обнаружить сетевую плату (рис. 15-1). Если у вас есть дискета с драйверами для данной платы, вставьте ее в дисковод. В противном случае ОС сама может предложить вставить диск с драйверами.

Рис. 15-1. Windows 2000 автоматически обнаруживает устройства Plug and Play.

3. Если ОС не обнаружила плату автоматически, см. пояснения в главе 2.
4. Если сетевые службы еще не установлены в ОС, читайте дальше.

Установка протокола TCP/IP

Протокол TCP/IP устанавливается либо автоматически при установке Windows 2000 либо из оснастки Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Если вы устанавливаете TCP/IP после установки Windows 2000, войдите в систему по учетной записи с привилегиями администратора и сделайте так.

1. В меню Start\Settings (Пуск\Настройка) выберите команду Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Откроется одноименное диалоговое окно (рис. 15-2).
2. Локальные соединения (Local area network connections, LAN connections) создаются автоматически, если на компьютере установлена сетевая плата и он подключен к сети. Если сетевых плат несколько, то для каждой из них будет создано по одному локальному соединению. Если сеть недоступна, нужно подключить компьютер к сети или создать альтернативный тип соединения (см. раздел «Управление сетевыми соединениями» этой главы).
3. Каждое сетевое соединение настраивается отдельно. Щелкните сетевое соединение правой кнопкой и из контекстного меню выберите команду Properties (Свойства). Откроется диалоговое окно свойств локального соединения.

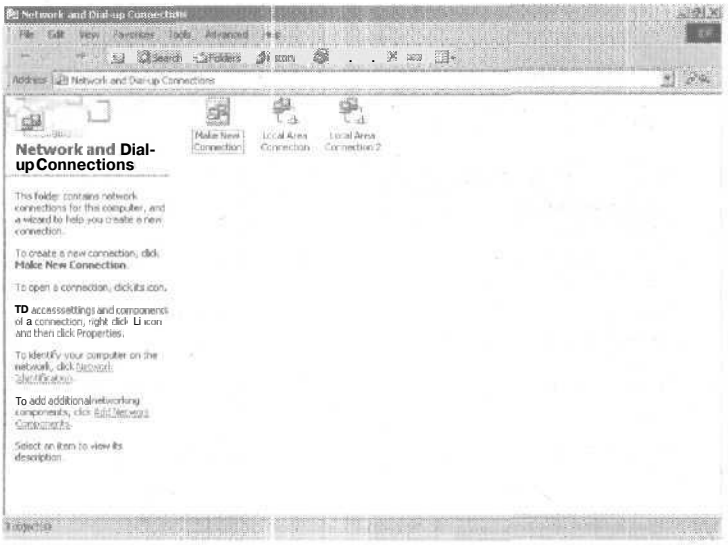


Рис. 15-2. Окно Network And Dial-Up Connections служит для управления сетевыми соединениями. Каждой сетевой плате соответствует одно локальное соединение.

4. Протокола TCP/IP нет в списке установленных компонентов, следовательно, его нужно установить. Щелкните кнопку Install, затем Protocol (Протокол) и затем — Add (Добавить). В диалоговом окне Select Network Protocol (Выбор сетевого протокола) выберите пункт Internet Protocol (TCP/IP) и щелкните OK.
5. Убедитесь, что выбран флажок Internet Protocol (TCP/IP), и щелкните OK.
6. Читайте следующий раздел — о настройке TCP/IP.

Настройка сети TCP/IP

Для передачи информации по сети TCP/IP используютея IP-адреса, которые в Windows 2000 можно настроить динамически и вручную.

- **Динамически** Если в сети установлен сервер DHCP (Dynamic Host Configuration Protocol), то назначение адресов может происходить динамически при загрузке

компьютера. *Динамические* (dynamic) адреса могут изменяться. Данный способ назначения IP-адресов является стандартной конфигурацией и в большинстве случаев автоматически настраивается Windows 2000 Professional.

- Вручную IP-адрес, назначенный вручную, называется *статическим* (static). Статический адрес не изменяется. Статические IP-адреса обычно назначаются серверам Windows 2000. При использовании статических IP-адресов нужно указать дополнительную информацию, которая поможет серверу ориентироваться в сети.

Настройка статических IP-адресов

Назначая статический IP-адрес, нужно указать еще и маску подсети и, если необходимо, шлюз по умолчанию, используемый при межсетевых коммуникациях. IP-адрес — это числовой идентификатор компьютера. Схемы адресации зависят от способа организации сети. Обычно IP-адрес выделяется из некоторого блока адресов, назначенного данному сегменту сети. Так, если компьютер находится в сегменте сети с адресом 192.168.10.0, то его IP-адрес лежит в диапазоне 192.168.10.1 - 192.168.10.254. Адрес 192.168.10.255 обычно резервируется для широковещательных сообщений.

Если локальная сеть подключена к Интернету напрямую, IP-адреса, назначаемые компьютерам, должны быть уникальны. Если сеть является частной и не имеет прямого выхода в Интернет, следует использовать частные IP-адреса (табл. 15-1).

Табл. 15-1. Адреса частной сети

Идентификатор частной сети	Маска подсети	Диапазон IP-адресов
10.0-0-0	255.0.0.0	10.0.0.1 - 10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1 - 172.31.255.254
192 168.0 0	255.255 0.0	192 168.255.254

Все остальные адреса являются общедоступными и должны быть арендованы или куплены.

Использование утилиты Ping для проверки адресов

Прежде чем назначить IP-адрес, нужно убедиться в том, что он свободен (не используется и не зарезервирован службой DHCP). Это позволяет сделать утилита Ping. Открыв окно

командной строки, наберите **ping** и нужный IP-адрес. Например, чтобы проверить адрес 192.168.10.12, введите команду:

```
ping 192.168.10.12
```

Назначение статического IP-адреса

Статические IP-адреса назначаются так.

1. В меню Start\Settings (Пуск\Настройка) выберите команду Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Откроется одноименное диалоговое окно.
2. Щелкните нужное сетевое соединение правой кнопкой и из контекстного меню выберите команду Properties (Свойства). Откроется диалоговое окно свойств локального соединения (рис. 15-3). Вид окна может слегка измениться, если вы не используете Internet Connection Sharing.

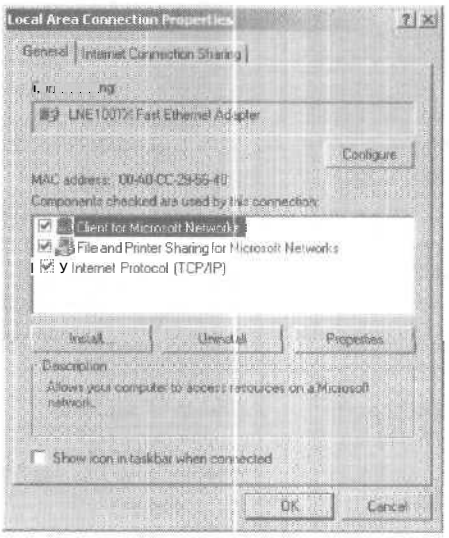


Рис. 15-3. Список установленных сетевых компонентов в окне свойств локального соединения.

3. Дважды щелкните пункт Internet Protocol (TCP/JP). Откроется диалоговое окно свойств TCP/IP (рис. 15-4),

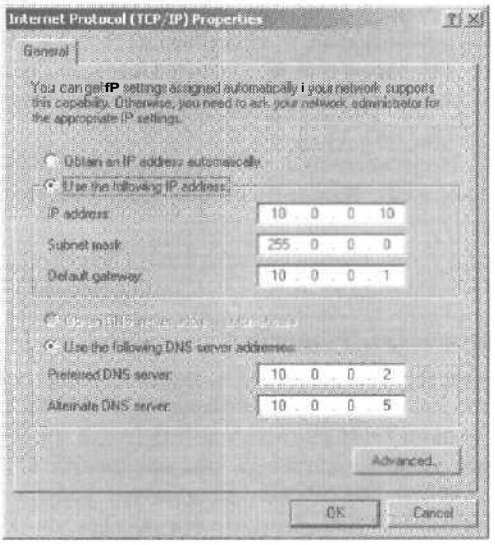


Рис. 15-4. Диалоговое окно свойств TCP/IP служит для настройки динамических и статических IP-адресов.

Примечание Локальные соединения создаются автоматически при загрузке компьютера, подключенного к сети. Для каждой сетевой платы, установленной на компьютере, будет показано по одному соединению. Другие типы соединений, например, телефонные, нужно создавать самостоятельно (см. раздел «Управление сетевыми соединениями» этой главы).

4. Щелкните переключатель Use The Following IP Address (Использовать следующий IP-адрес) и введите IP-адрес в поле IP Address (IP-адрес). Данный IP-адрес должен быть уникален в пределах вашей сети.
5. Маска подсети обеспечивает корректное взаимодействие компьютера с другими узлами сети. Windows 2000 должен вставить стандартное значение маски подсети в поле Subnet Mask (Маска подсети). Если сеть не состоит из подсетей, стандартное значение маски должно быть пустым. В противном случае нужно изменить стандартное значение, на то, которое соответствует вашей сети.

6. Если компьютер должен иметь доступ к другим подсетям, Интернету и другим сетям TCP/IP, нужно настроить шлюз по умолчанию. Для этого в поле Default Gateway (Шлюз по умолчанию) введите IP-адрес маршрутизатора по умолчанию вашей сети.
7. Щелкните OK. Повторите эти действия для всех настраиваемых сетевых плат. Каждой сетевой плате требуется уникальный IP-адрес.
8. При необходимости настройте службы DNS (Domain Name Service) и WINS (Windows Internet Naming Service).

Настройка динамических IP-адресов

Служба DHCP обеспечивает централизованное управление IP-адресами и стандартными параметрами TCP/IP. Если в сети установлен сервер DHCP, то каждой сетевой плате на любом компьютере можно назначить динамический IP-адрес. Кроме того, сервер DHCP автоматизирует работу и с другими параметрами TCP/IP. Динамическую адресацию не следует применять для серверов Windows 2000, так как динамические IP-адреса могут изменяться. Динамическая адресация настраивается так.

1. В меню Start\Settings (Пуск\Настройка) выберите команду Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Откроется одноименное диалоговое окно.
2. Щелкните нужное сетевое соединение правой кнопкой и из контекстного меню выберите команду Properties (Свойства). Если соединение недоступно, см. раздел «Управление сетевыми соединениями» этой главы.
3. Дважды щелкните Internet Protocol (TCP/IP). Откроется диалоговое окно свойств TCP/IP.
4. Выберите переключатель Obtain An IP Address Automatically (Получить IP-адрес автоматически).

Примечание Каждой сетевой плате соответствует одно локальное соединение. Такие соединения создаются автоматически.

5. При необходимости отметьте флажок Obtain DNS Server Address Automatically (Получить адрес DNS-сервера автоматически).
6. Щелкните OK.

Настройка нескольких IP-адресов и шлюзов

Компьютер Windows 2000 может поддерживать несколько IP-адресов даже при наличии единственной сетевой платы. Несколько IP-адресов полезно иметь в следующих ситуациях.

- Компьютер должен выступать в роли нескольких компьютеров. Например, сервер поддерживает службы Web, FTP (File Transfer Protocol) и SMTP (Simple Mail Transfer Protocol). Для каждой из этих служб можно использовать различные IP-адреса.
- Сеть разбита на несколько логических сетей (подсетей), и компьютер должен иметь доступ к каждой из них. В этом случае одной сетевой плате можно назначить несколько IP-адресов, например, адресу 192.168.10.8 будет доступен для рабочих станций из подсети 192.168.10.0, а адрес 192,168.11.8 - из подсети 192.168.11.0.

Внимание! Если сетевая плата одна, IP-адреса должны принадлежать сегменту или сегментам одной локальной сети. Если сеть разбита на несколько физических сетей, требуется несколько плат, каждой из которых будет назначен IP-адрес, соответствующий отдельному сегменту сети.

Назначение адресов и шлюзов

Каждая сетевая платаможет иметь один или несколько IP-адресов. Эти адреса могут быть связаны с одним/несколькими стандартными шлюзами. Чтобы назначить одной сетевой плате несколько IP-адресов и шлюзов, сделайте так.

1. В меню Start\Settings (Пуск\Настройка) выберите команду Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Откроется одноименное диалоговое окно.
2. Щелкните нужное сетевое соединение правой кнопкой и из контекстного меню выберите команду Properties (Свойства). Если соединение недоступно, см. раздел «Управление сетевыми соединениями» этой главы.
3. Дважды щелкните Internet Protocol (TCP/IP). Откроется диалоговое окно свойств TCP/IP.
4. Щелкните кнопку Advanced (Дополнительно), откроется окно Advanced TCP/IP Settings (рис. 15-5).
5. Выберите вкладку IP Settings в области IP Addresses щелкните кнопку Add (Добавить) и в полях IP Address

(IP-адрес) и Subnet Mask (Маска подсети) введите IP-адрес и маску подсети. Выполните эти действия для каждого IP-адреса, который нужно назначить сетевой плате.

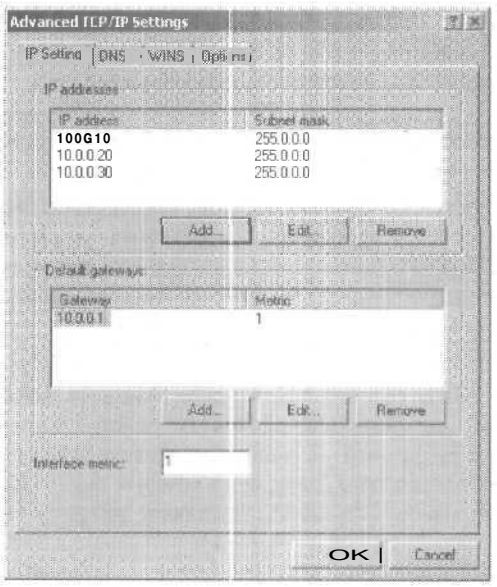


Рис. 15-5. Диалоговое окно Advanced TCP/IP Settings позволяет настроить несколько IP-адресов и шлюзов.

6. Вы можете указать и дополнительные шлюзы: щелкнув кнопку Add (Добавить), введите в полях Gateway (Шлюз) и Metric (Метрика) адрес шлюза и метрику. Повторите эти действия для каждого нужного вам шлюза.

Совет Метрика обозначает относительную стоимость использования шлюза. Если для IP-адреса указано несколько шлюзов по умолчанию, то в первую очередь используется шлюз с наименьшей метрикой. Если связь с ним установить не удается, Windows 2000 пытается соединиться со следующим шлюзом.

Настройка разрешения DNS

DNS — служба разрешения имен — предназначена для определения IP-адреса компьютера по его имени. Она позво-

ляет использовать имена узлов, например *http://www.msn.com* или *http://www.microsoft.com* вместо IP-адресов (192.168.5.102 и 192.168.12.68). DNS является основной службой имен для Windows 2000 и Интернет.

Совет Для работы DNS в сети нужно установить сервер DNS. Об управлении серверами DNS см. главу 19.

Основные **параметры** службы DNS

Основные параметры службы DNS настраиваются так.

1. В меню Start\Settings (Пуск\Настройка) выберите команду Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Откроется одноименное диалоговое окно.
2. Щелкните нужное сетевое соединение правой кнопкой и из контекстного меню выберите команду Properties (Свойства). Если соединение недоступно, см, раздел «Управление сетевыми соединениями» этой главы.
3. Дважды щелкните пункт Internet Protocol (TCP/IP). Откроется диалоговое окно свойств TCP/IP.
4. Если компьютер использует службу DHCP и вы хотите применять се для определения адресов серверов DNS, выберите переключатель Obtain DNS Server Address Automatically (Получить адрес DNS-сервера автоматически). В противном случае выберите переключатель Use The Following DNS Server Addresses (Использовать следующие адреса DNS-серверов) и введите адреса основного и дополнительного серверов DNS.

Дополнительные параметры **службы DNS**

Для настройки дополнительных параметров службы DNS предназначена вкладка DNS в окне Advanced TCP/IP Settings (рис. 15-6). На ней доступны следующие поля.

- DNS Server**Addresses,** In Order Of Use Определяет IP-адреса серверов DNS, используемых для разрешения имен доменов. Кнопки Add (Добавить), Remove (Удалить) и Edit (Изменить) позволяют соответственно добавить, удалить и редактировать список серверов. Для разрешения имен можно использовать несколько серверов, при этом их приоритет определяется порядком следования в списке. Если первый сервер не может ответить на запрос разрс-

шения имени домена, запрос посылается на второй и т. д. Помните, что TCP/IP отправляет запрос на следующий сервер, только если предыдущий не отвечает, но никак не из-за того, что тот не смог разрешить указанное имя. Кнопки со стрелками позволяют изменить положение сервера в списке.

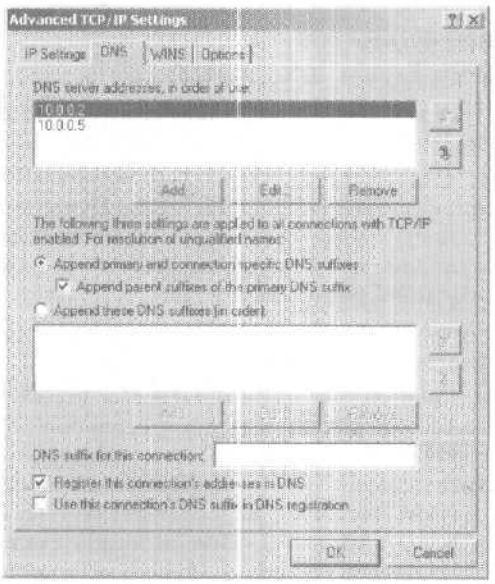


Рис. 15-6. Вкладка DNS диалогового окна Advanced TCP/IP Settings позволяет настроить дополнительные параметры службы DNS.

- **Append Primary And Connection Specific DNS Suffixes** Этот переключатель (по умолчанию включен) служит для разрешения неполных имен компьютеров в основном домене. Так, если компьютер «Rage» расположен в родительском домене microsoft.com, его имя будет преобразовано в rage.microsoft.com. Если полного доменного имени нет в родительском домене, запрос разрешения имени не выполнится. Родительские домены определяются на вкладке Network Identification диалогового окна System Properties.

- Append Parent Suffixes Of The Primary DNS Suffix Этот флажок (по умолчанию отмечен) применяется для разрешения неполных доменных имен в иерархии родительский—дочерний. Если имя не удастся разрешить в данном домене, к нему добавляется суффикс родительского домена. Так продолжается, пока не будет достигнута вершина иерархии. Например, если компьютер «Rage» расположен в домене dev.microsoft.com, служба DNS сначала попытается разрешить имя rage.dev.microsoft.com, а в случае неудачи — rage.microsoft.com.
- Append These DNS Suffixes (In Order) Этот флажок позволяет задать конкретные суффиксы DNS, используемые при разрешении имен вместо суффикса родительского домена. Кнопки Add (Добавить), Remove (Удалить) и Edit (Изменить) позволяют соответственно добавить, удалить и редактировать список суффиксов. Для разрешения имен можно использовать несколько суффиксов, при этом их приоритет определяется порядком следования в списке. Если запрос разрешения имени не выполняется с применением первого суффикса, используется второй и т. д. Кнопки со стрелками позволяют изменить положение суффикса в списке.
- DNS Suffix For This Connection Определяет суффикс DNS для соединения, который заменяет доменные имена, уже настроенные для данного соединения. Обычно доменное имя указывают на вкладке Network Identification в окне System Properties.
- RegisterThis Connection's Addresses In DNS Этот флажок (по умолчанию отмечен) позволяет зарегистрировать в DNS все IP-адреса данного соединения под полным доменным именем данного компьютера.
- **Use This Connection's DNS Suffix In DNS Registration** Этот флажок позволяет зарегистрировать в DNS все IP-адреса данного соединения под именем родительского домена.

Настройка разрешения WINS

Служба WINS преобразует имена компьютеров NetBIOS в IP-адреса. Кроме того, она помогает компьютерам определять адреса других компьютеров в сети. Для работы службы в сети

нужно установить сервер WINS. Службу WINS поддерживают все версии Windows, поэтому Windows 2000 использует ее из соображений совместимости.

Для разрешения имен NetBIOS Windows 2000 может также использовать локальный файл LMHOSTS. Однако LMHOSTS применяется только когда нормальные методы разрешения имен не срабатывают. В грамотно настроенной сети эти файлы практически не используются. Так что основным методом разрешения имен NetBIOS является служба WINS.

Служба WINS настраивается так.

1. Откройте диалоговое окно Advanced Internet Protocol (TCP/IP) Properties и выберите вкладку WINS (рис. 15-7).

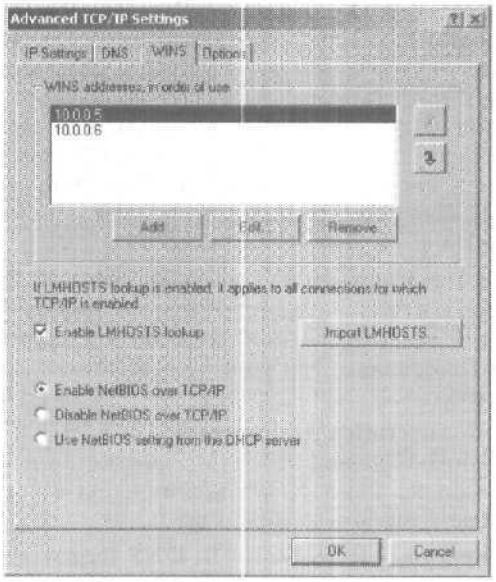


Рис. 15-7. Вкладка WINS диалогового окна Advanced TCP/IP Settings позволяет настроить службу WINS.

2. В списке WINS Addresses, In Order Of Use перечислены IP-адреса серверов WINS, которые используются для разрешения имен NetBIOS. Кнопки Add (Добавить), Remove (Удалить) и Edit (Изменить) позволяют соответственно добавить, удалить и редактировать список серверов.

3. Для разрешения имен NetBIOS можно использовать несколько серверов WINS, при этом их приоритет определяется порядком следования в списке. Если первый сервер WINS не может ответить на запрос разрешения имени NetBIOS, запрос посылается на второй и т. д. Помните, что TCP/IP отправляет запрос на следующий сервер, только если предыдущий не отвечает, но никак не из-за того, что тот не смог разрешить указанное имя. Чтобы изменить положение сервера в списке, воспользуйтесь стрелками.
4. Чтобы включить поиск по файлу LMHOSTS, отметьте флажок Enable LMHOSTS Lookup. Если вы хотите, чтобы компьютер использовал файл LMHOSTS, находящийся в определенном месте сети, укажите его с помощью кнопки Import LMHOSTS. В основном файлы LMHOSTS применяются только при отказе других методов разрешения имен.

Примечание Файлы LMHOSTS хранятся на разных компьютерах и поэтому ненадежны. Не полагайтесь на них — лучше проверьте правильность настройки и доступность серверов DNS и WINS, которые обеспечивают централизованное администрирование службами разрешения имен.

5. Для разрешения имен WINS требуются службы NetBIOS Over TCP/IP. При использовании службы DHCP и динамической адресации можно загружать параметры NetBIOS с DHCP-сервера. Для этого нужно отметить флажок Use NetBIOS Setting From The DHCP Server. В противном случае нужно включить или отключить NetBIOS с помощью переключателей Enable NetBIOS Over TCP/IP и Disable NetBIOS Over TCP/IP
6. Повторите эту процедуру для других сетевых плат.

Настройка дополнительных сетевых компонентов

Windows 2000 предоставляет большое количество дополнительных сетевых клиентов, служб и протоколов. Для установки дополнительных сетевых компонентов предназначены диалоговое окно Network Connection Properties и мастер Windows Optional Networking Components Wizard.

Установка и удаление сетевых компонентов

Для установки сетевых клиентов, служб и протоколов предназначено диалоговое окно Network Connection Properties (табл. 15-2). Некоторые компоненты доступны только на серверах Windows 2000.

Табл. 15-2. Сетевые компоненты Windows 2000

Компонент	Описание
Клиент для сетей Microsoft (Client for Microsoft Networks)	Позволяет компьютеру работать с ресурсами сетей Windows.
Gateway (and Client) Services for NetWare	Позволяет компьютеру работать с ресурсами сетей NetWare.
Служба доступа к файлам и принтерам сетей Microsoft (File and Printer Sharing for Microsoft Networks)	Позволяет другим узлам работать с ресурсами данного компьютера.
Протокол AppleTalk (AppieTalk Protocol)	Позволяет другим узлам взаимодействовать с данным компьютерам но протоколу AppleTalk. Позволяет серверам Windows 2000 функционировать как маршрутизаторам AppleTalk.
NWLink NetBIOS	Позволяет компьютеру взаимодействовать с серверами NetWare через протокол NetBIOS.
Совместимый транспортный протокол NWLink IPX/SPX/ NetBIOS (NWLink IPX/SPX/ NetBIOS Compatible Transport Protocol)	Позволяет компьютеру взаимодействовать с серверами NetWare через протокол IPX/SPX.
Драйвер сетевого монитора (Network Monitor Driver)	Драйвер, позволяющий утилите Netmon (сетевому монитору) собирать пакеты, передаваемые но сети.
Планировщик пакетов QoS (QoS Packet Scheduler)	Планировщик пакетов Quality of Service, предоставляющий службы управления сетевым трафиком.
Агент SAP (SAP Agent)	Протокол SAP (Service Advertising Protocol) позволяет «рекламировать» сервера и адреса в сети.

Табл. 15-2. Сетевые компоненты Windows 2000

Компонент	Описание
Протокол DLC	Протокол DLC (Data Link Control) позволяет компьютеру подключаться к большим компьютерам IBM.
Протокол NetBEUI	Расширенный пользовательский интерфейс NetBIOS (NetBIOS Enhanced User Interface) — стандартный протокол фирмы Microsoft для передачи данных в сетях Windows NT.

Любой из перечисленных выше компонентов можно установить/удалить.

1. В меню Start\Settings (Пуск\Настройка) выберите команду Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Откроется одноименное диалоговое окно.
2. Щелкните нужное сетевое соединение правой кнопкой и из контекстного меню выберите команду Properties (Свойства). Если соединение недоступно, см. раздел «Управление сетевыми соединениями» этой главы,
3. Откроется диалоговое окно Network Connection Properties со списком установленных компонентов.
4. Чтобы отключить компонент, снимите связанный с ним флажок.
5. Чтобы удалить компонент, выберите его и щелкните кнопку Uninstall (Удалить). В открывшемся диалоговом окне щелкните кнопку Yes (Да), чтобы подтвердить удаление.
6. Чтобы установить компоненты, щелкните кнопку Install (Установить). Откроется диалоговое окно Select Network Component Type (Выбор типа сетевого компонента). Выберите тип компонента (Client, Protocol или Service) и щелкните кнопку Add (Добавить). Выберите нужный компонент.

Установка дополнительных сетевых компонентов

Для установки дополнительных сетевых компонентов предназначен мастер Windows Optional Networking Components Wizard. Кроме компонентов Windows 2000, может понадобиться установить утилиты, необходимые для их работы. Эти утилиты устанавливаются в общую папку Administrative Tools.

Ниже представлен обзор дополнительных сетевых компонентов (табл. 15-3). Имена пакетов компонентов перечислены в окне Windows Comporents. Имена отдельных компонентов можно увидеть, щелкнув кнопку Detail. Некоторые компоненты доступны только на серверах Windows 2000.

Дополнительные сетевые компоненты устанавливают так:

1. В меню Start\Settings (Пуск\Настройка) выберите команду Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Откроется одноименное диалоговое окно.
2. Щелкните кнопку Add Network Components. Запустится мастер Windows Optional Networking Components Wizard. Щелкните кнопку Next (Далее).
3. Откроется диалоговое окно со списком пакетов компонентов: Management And Monitoring Tools, Networking Services и Other Network File And Print Services (рис. 15-8).

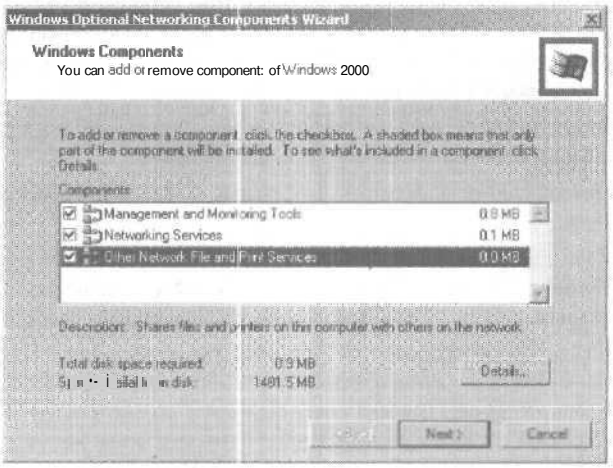


Рис. 15-8. Выберите нужный пакет компонентов. Щелкните кнопку Details, чтобы установить отдельные компоненты.

4. Чтобы установить или удалить отдельные компоненты пакета, выберите нужный пакет и щелкните кнопку Details.
5. Щелкните OK, затем Next (Далее). Выбранные компоненты будут установлены.

Управление сетевыми соединениями

Удаленные и сетевые соединения позволяют получить доступ к ресурсам на удаленных компьютерах. Этот раздел посвящен созданию и управлению сетевыми соединениями. Локальные соединения создаются автоматически при загрузке компьютера, подключенного к сети, поэтому этот тип соединений не нужно создавать вручную.

Создание сетевых соединений

Windows 2000 позволяет настроить большое количество различных удаленных и сетевых соединений. Соединение создается так.

1. В меню Start\Settings (Пуск\Настройка) выберите команду Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Откроется одноименное диалоговое окно.
2. Дважды щелкните значок Make New Connection (Создать новое соединение). Запустится мастер Network Connection Wizard. Щелкните кнопку Next (Далее). При необходимости укажите телефонный код области и способ набора номера.
3. Выберите нужный тип соединения (рис. 15-9).
   - Dial-Up To Private Network позволяет организовать удаленный доступ к корпоративной сети. При удаленном доступе используются модемы или ISDN-линии (Integrated Services Digital Network).
   - Dial-Up To The Internet позволяет организовать удаленный доступ в Интернет. При удаленном доступе используются модемы или ISDN-линии. После подключения к поставщику услуг Интернета соединение можно сделать общим для других компьютеров.
   - **Connect To A Private Network Through The Internet** позволяет организовать защищенное соединение с корпоративной сетью через Интернет. В защищенных VPN-соединениях используются протоколы PPTP (Point To Point Tunneling Protocol) или L2TP (Layer 2 Tunneling Protocol).
   - Accept Incoming Connections позволяет организовать доступ через входящие соединения, используя службы удаленного доступа. Если компьютер поддержива-

Табл. 15-3. Дополнительные сетевые компоненты Windows 2000.

Пакет компонентов	Имя отдельного компонента	Описание
Средства управления и мониторинга (Management And Monitoring Tools)	Диспетчер соединений (Connection Manager Components)	Устанавливает пакет Диспетчер соединений (Connection Manager) и службу Адресная книга (Phone Book).
	Средства мониторинга сети (Network Monitoring Tools)	Устанавливает средства мониторинга сети, позволяющие анализировать сетевой трафик.
	Протокол SNMP (Simple Network Management. Protocol)	Устанавливает агентов SNMP и SNMP.
Сетевые службы (Networking Services)	COM Internet Services Proxy	Позволяет COM-объектам (Component Object Model) взаимодействовать через HTTP (Hypertext Transfer Protocol).
	Служба DNS (Domain Name System)	Позволяет компьютеру функционировать как DNS-сервер.
	Протокол DHCP (Dynamic Host Configuration Protocol)	Позволяет компьютеру функционировать как DHCP-сервер.
	Служба аутентификации н Интернет *(Internet* Authentication Service)	Обеспечивает аутентификацию, авторизацию и поддержку учетных записей для удаленных пользователей и пользователей виртуальных частных сетей (Virtual Private Network, VPN).
	Служба управления доступом QoS (QoS Admission Control Service)	Позволяет управлять качеством сетевых соединений.
	Основные службы TCP/IP (Simple TCP/IP Services) и Quote of the Day.	Устанавливает основные службы TCP/IP: Character Generator, Daytime, Discard, Echo

Табл. 15-3. *(продолжение)*

Пакет компонентов	Имя отдельного компонента	Описание
	Службы Site Server ILS (Site Server ILS Services)	Позволяют серверу сайта обновлять информацию R каталоге.
	Служба WINS (Windows Internet. Naming Service)	Позволяет компьютеру функционировать как WINS-сервер.
Другие сетевые службы доступа к файлам и принтерам (Other Network File And Print. Services)	Службы доступа к файлам для Macintosh (File Services for Macintosh)	Позволяет пользователям компьютеров Macintosh работать с файлами па сервере Windows 2000.
	Службы доступа к принтерам для Macintosh (Print Services tor Macintosh)	Позволяет пользователям компьютеров Macintosh посылать задания печати на принтер, подключенный к серверу Windows 2000.
	Службы доступа к принтерам для Unix (Print Services for Unix)	Позволяет пользователям компьютеров Unix посылать задания печати на принтер, подключенный к серверу Windows 2000.

ет VPN, прямые и удаленные соединения, необходимо также настроить поддержку входящих соединений.

- Connect Directly To Another Computer позволяет организовать прямое соединение с другим компьютером через последовательный, параллельный или инфракрасный порт. Например, такое соединение применяется для подключения к ПК портативного компьютера.

4. Откроется диалоговое окно, вид которого зависит от выбранного вами типа соединения. Выполните инструкции, предложенные в каждом окне. Щелкните кнопку Finish (Готово). Соединение будет создано.

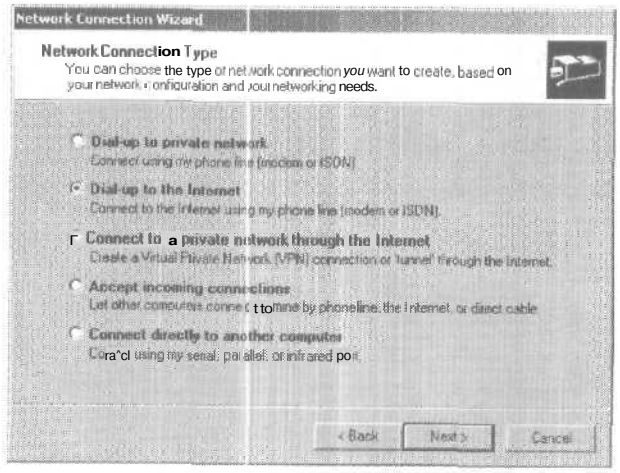


Рис. 15-9. Типы соединений.

Включение и отключение сетевых соединений

Локальные соединения создаются и активизируются автоматически. Новое соединение можно отключить/создать.

1. В меню Start\Settings (Пуск\Настройка) выберите команду Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Откроется одноименное диалоговое окно.
2. Чтобы отключить соединение, щелкните его правой кнопкой и из контекстного меню выберите команду Disconnect (Отключить).

3. Чтобы включить соединение, щелкните его правой кнопкой и из контекстного меню выберите команду Connect (Включить).

Удаление сетевых соединений

Ненужное сетевое соединение можно удалить.

1. В меню Start\Settings (Пуск\Настройка) выберите команду Network And Dial-Up Connections (Сеть и удаленный доступ к сети). Откроется одноименное диалоговое окно.
2. Щелкните соединение правой кнопкой и из контекстного меню выберите команду Delete (Удалить). Щелкните кнопку Yes (Да), чтобы подтвердить удаление.

Примечание Локальные **сетевые** соединения удалить невозможно, а их управлением занимается **ОС** Windows 2000.

Изменение и дублирование соединений

Чтобы изменить свойства соединения, щелкните его правой кнопкой и из контекстного меню выберите команду Properties (Свойства). Прежде, чем вносить изменения в параметры текущего соединения, сделайте его копию. Для этого, щелкнув нужное соединение правой кнопкой, выберите из контекстного меню команду Create Copy (Создать копию). Windows 2000 позволяет делать копии любых созданных ранее (т. с, не локальных) соединений.

Проверка конфигурации TCP/IP

После установки ОС или изменения конфигурации, работоспособность компьютера следует протестировать. Самый простой способ проверки параметров TCP/IP — дать команду PTNG:

ping *узел*

где *узел* — имя узла.

Утилиту Ping можно запустить несколькими способами.

- **Попытаться** опросить **IP-адреса** компьютеров. Если компьютер настроен правильно и нужный узел доступен в сети, на запрос утилиты Ping должен прийти ответ. В противном случае утилита сообщит о том, что время ожидания истекло.

- **В доменах,** поддерживающих **службу WINS, попытаться опросить имена компьютеров NetBIOS.** Если имена компьютеров NetBIOS разрешаются правильно, то такие средства NetBIOS, как служба WINS, настроены должным образом.
- **В доменах, поддерживающих службу DNS, попытаться опросить имена узлов DNS.** Если полные имена узлов DNS разрешаются правильно, то служба DNS настроена должным образом.

Кроме конфигурации TCP/IP можно протестировать поиск компьютера в сети. Для этого компьютер должен быть членом домена Windows 2000, в котором разрешен поиск компьютеров. Войдите в систему, откройте Windows Explorer или My Network Places и попробуйте найти другие компьютеры домена. После этого войдите в другой компьютер и попытайтесь найти тот, который вы только что настроили. Если эти тесты выполняются, то разрешение DNS в локальном окружении настроено правильно. В противном случае нужно проверить параметры службы DNS и протоколов.

Глава 16

Управление сетевыми принтерами и службами доступа к принтерам

Чтобы предоставить удаленным пользователям доступ к печатающему устройству, подключенному к компьютеру с Microsoft Windows 2000, администратор должен сделать две вещи: настроить компьютер как сервер печати и задействовать его для совместного использования печатающих устройств в сети.

Эта глава посвящена настройке, предоставлению доступа, администрированию и устранению неполадок, связанных с работой общих принтеров, В главе не рассматривается печать через Интернет.

Примечание В Windows 2000 термины, связанные с принтерами и печатающими устройствами, несколько отличаются от общепринятых. Термин *печатающее устройство* (print device) обозначает физическое устройство, которое осуществляет вывод на печать. Печатающие устройства, подключенные к серверам печати, называются локальными. Устройства, подключенные к сети напрямую, называются сетевыми. *Принтером* (printer) называется ПО, отвечающее за взаимодействие ОС и печатающего устройства. Принтеры устанавливаются на серверах печати. Заметьте: в документации и диалоговых окнах эти термины часто считаются взаимозаменяемыми. В этом случае нужно попытаться понять, что имели в виду разработчики: физическое устройство («печатающее устройство») или ПО («принтер»).

Устранение неполадок в работе принтера

Знание принципов работы принтера сэкономит долгие часы устранения неполадок в их работе. При печати документа взаимодействует множество процессов, драйверов и аппаратных устройств. Если принтер подключен к серверу печати, процесс печати состоит в следующем.

- **Драйвер принтера.** Когда документ посылается на печать, загружается драйвер принтера. Он загружается с локального или удаленного компьютера в зависимости от того, куда подключено печатающее устройство. Доступность драйвера принтера на удаленном компьютере зависит от ОС и архитектуры процессора. Если компьютер не может получить последнюю версию драйвера принтера, это, возможно, связано с тем, что администратор не включил драйвер принтера для данной ОС. Подробнее об этом см. раздел «Управление драйверами принтера».
- **Локальный** спулер **и процессор печати.** Приложение, посылающее документ на печать, использует драйвер принтера для преобразования документа в формат, понятный печатающему устройству. Затем компьютер отправляет документ в локальный спулер печати, который передает его процессору печати, где создаются предварительные данные, необходимые печатающему устройству для печати документа.
- **Маршрутизатор** и спулер печати на **сервере** печати. Предварительные данные посылаются обратно в локальный спулер печати. Если печать осуществляется с удаленного компьютера, данные направляются в спулер сервера печати. В Windows 2000 маршрутизатором печати является программа WINSPOOL.EXE, в задачи которой входит поиск удаленного принтера, управление заданиями печати и загрузка драйверов принтера. Обычно в невыполнении любой из этих задач виноват именно маршрутизатор печати. Об исправлении неполадок, связанных с работой маршрутизатора печати, см. разделы «Решение проблем буферизации» и «Настройка разрешений доступа к принтерам». Если предложенные в них способы решения неисправностей не помогут, можно попробовать заменить или восстановить файл WINSPOOL.EXE.

Основная идея загрузки драйверов с удаленного компьютера в том, что при обновлении драйвера принтера, вам не нужно устанавливать новую версию на всех компьютерах сети — достаточно заменить драйвер только на сервере печати. Подробнее об этом см. раздел «Управление драйверами принтера».

- Принтер **(очередь печати).** Из спулера печати документ попадает в стек печати (в некоторых ОС — очередь печати) печатающего устройства. Документ, находящийся в очереди печати, называют *заданием печати* (print job). Время нахождения документа в очереди печати зависит от его приоритета и позиции. Подробнее об этом см. раздел «Настройка времени и приоритета заданий печати».
- **Монитор печати.** Когда подходит очередь печати документа, монитор печати отправляет его на печатающее устройство. Принтер можно настроить так, чтобы он сообщал пользователю о завершении печати документа.

  Монитор принтера, используемый ОС Windows 2000, зависит от конфигурации и типа печатающего устройства. Стандартным монитором печати является файл LOCALMON.DLL. Производители печатающих устройств часто разрабатывают собственные мониторы печати, например, HPMON.DLL, применяемый устройствами компании Hewlett-Packard. Эта динамическая библиотека (dynamic link-library, DLL) необходима для печати документов на данных печатающих устройствах. В случае повреждения или отсутствия ее нужно переустановить.
- **Печатающее** устройство. Печатающим называют устройство, предназначенное для печати документа на бумаге. Чаще всего при работе с печатающим устройством встречаются следующие ошибки.
  - **Insert Paper Into Tray X.** Печатающее устройство не может найти бумагу в специальном лотке. Поместите ее туда.
  - **Low Toner.** Когда в печатающем устройстве кончается красящий порошок, можно попробовать вынуть картридж, встряхнуть его несколько раз и вставить обратно. При встряхивании картриджа порошок перемешиваются, что часто позволяет напечатать несколько дополнительных страниц.

- **Out Of Paper.** В печатающем устройстве закончилась бумага. Поместите бумагу в лоток.
- **Out Of Toner; Out Of Ink.** В печатающем устройстве закончились чернила или красящий порошок. Вставьте новый картридж.
- **Paper Jam.** Бумага застряла в печатающем устройстве. Откройте корпус, выньте застрявшую бумагу и снова включите устройство.
- Printer **Off-Line.** Печатающее устройство разогревается или находится в процессе инициализации. Подождите немного.

Право установки и управления принтерами определяется групповой политикой. Если у вас возникают проблемы при работе с принтером и вы полагаете, что они связаны с групповой политикой, проверьте ее настройку в:

- Computer Configuration\Printers **(Конфигурация** компьютера\Принтеры);
- User Configuration\Control Panel\Printers (Конфигурация пользователя\Панель управления\Принтеры);
- **User** Configuration\Start Menu & Taskbar (Конфигурация пользователя\Главное меню **и Панель** задач).

Установка принтеров

Windows 2000 позволяет устанавливать (управлять) принтеры в (из) любой точки сети. Для установки (управления) принтеров служит панка Printers (Принтеры). Чтобы открыть эту папку на локальном компьютере, выберите в меню Start\Settings (Пуск\Настройка) команду Printers. На удаленном компьютере доступ к этой папке можно получить через My Network Places (Мое сетевое окружение): войдите в домен, выберите нужный компьютер и дважды щелкните значок Printers.

Использование локальных и сетевых принтеров

Все печатающие устройства, подключенные к сети, делятся на два типа:

- **локальные** подключены непосредственно к компьютеру, к ним имеет доступ только тот пользователь, который на нем работает;

- **сетевые** — доступ к этим печатающим устройствам можно получить с удаленного компьютера; сетевое печатающее устройство может быть подключено к серверу печати или прямо к сети через сетевую плату.

Сетевые принтеры устанавливаются на серверах печати или как отдельные устройства, подключенные к сети. Сервер печати (print server) — это сервер или рабочая станция с Windows 2000, обеспечивающая совместное использование одного или нескольких принтеров, подключенных к компьютеру или сети.

Сервером печати может быть любая рабочая станция или сервер с Windows 2000. Его основная задача — управление общими печатающими устройствами и буферизацией печати. Основное преимущество серверов печати заключается в централизованном управлении очередью печати и отсутствии необходимости устанавливать драйверы принтера па компьютерах клиентов.

Примечание Серверы печати под Windows 2000 Professional поддерживают до 10 параллельных соединений и не могут обрабатывать запросы печати, поступающие от клиентов Macintosh и NetWare.

Однако использовать сервер печати не обязательно. Пользователи могут работать с принтерами, подключенными к сети напрямую. При этом работа с сетевым принтером во многом напоминает работу с локальным. Единственное отличие в том, что доступ к принтеру могут получить несколько пользователей, у каждого из которых будет своя очередь печати. Каждая очередь печати обслуживается отдельно, что может привести к трудностям при администрировании и устранении неполадок.

Чтобы установить или настроить новый принтер, нужно быть членом одной из привилегированных групп (табл. 16-1).

Чтобы подключиться и напечатать документ на принтере, нужно иметь соответствующие разрешения доступа. Подробнее об этом см. раздел «Настройка разрешений доступа к принтерам».

Табл. 16-1. Пользователи, обладающие правом настройки принтеров.

Группа	Windows 2000 Professional	Windows 2000 Server
Administrators	+	+
Power Users	+	
Print Operators		+
Server Operators		+

Установка печатающего устройства на локальном или удаленном сервере печати

Печатающее устройство на сервере печати устанавливают так.

1. Откройте папку Printers (Принтеры) на компьютере, который вы хотите сделать сервером печати. Доступ к этой папке можно получить как с локального, так и с удаленного компьютера. В первом случае в меню Start\Settings (Пуск\Настройка) зыберите команду Printers, а во втором — откройте My Network Places (Мое сетевое окружение), войдите в домен, выберите нужный компьютер и дважды щелкните значок Printers.

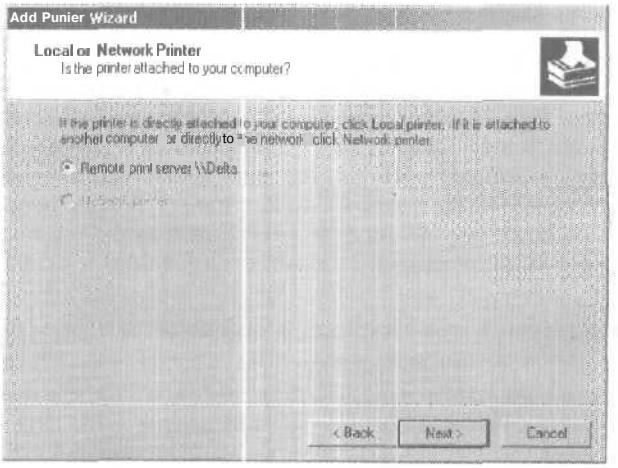


Рис. 16-1. Сервер печати можно настроить удаленно, но для этого придется выполнить несколько дополнительных действий.

2. Дважды щелкните значок Add Printer (Установка принтера). Запустится мастер Add Printer Wizard. Щелкните кнопку Next (Далее).
3. Если сервер печати настраивается удаленно, откроется диалоговое окно (рис, 16-1). По умолчанию отмечен переключатель Remote Print Server, Щелкните Next.
4. Если сервер печати настраивается локально, откроется диалоговое окно (рис. 16-2). Отметьте переключатель Local Printer (Локальный принтер), выберите автоматический поиск принтера и щелкните Next.
5. В процессе установки нового сетевого принтера Windows 2000 попытается автоматически обнаружить новое печатающее устройство, подключенное к локальному или удаленному серверу печати. Дальнейшие действия зависят от того, удалось ли системе обнаружить печатающее устройство.

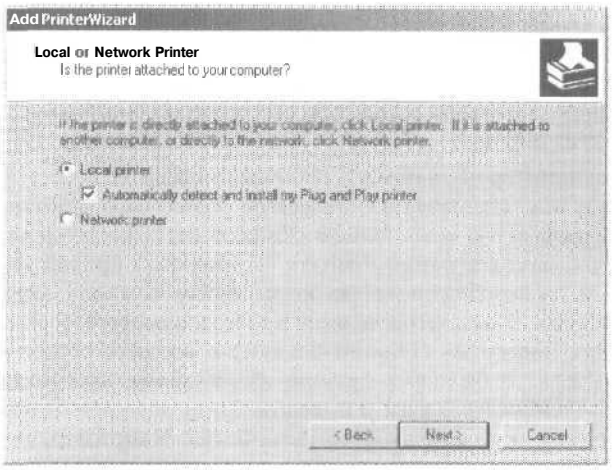


Рис. 16-2. Серверы печати можно настраивать локально.

Печатающее устройство обнаружено

Если ОС сможет обнаружить печатающее устройство, откроется диалоговое окно Found New Hardware (рис. 16-3). Windows 2000 начнет устанавливать повое устройство и необходимые драйверы. Если драйверы не будут найдены, ОС пред-

ложит вставить компакт диск с дистрибутивом Windows 2000 в привод CD-ROM или дискету в дисковод.

Рис. 16-3. Диалоговое окно Found New Hardware (Обнаружено новое устройство) говорит о том, что ОС смогла обнаружить новое печатающее устройство и начинается его установка.

Чтобы завершить установку, сделайте так.

1. После настройки печатающего устройства мастер Add Printer Wizard предложит напечатать пробную страницу. Щелкните кнопку Yes (Да), если хотите напечатать пробную страницу, и No (Нет) в противном случае.
2. Щелкните кнопку Next (Далее), а затем — Finish (Готово), чтобы завершить установку принтера. Имя и совместное использование принтера устанавливаются автоматически мастером Add Printer Wizard. По умолчанию именем принтера является его модель, например, HP DeskJet 890 C.
3. Если принтер подключен к рабочей станции Windows 2000. то после установки он становится локальным принтером и недоступен в сети. Чтобы сделать его общим, щелкните его значок в папке Printers (Принтеры) правой кнопкой и из контекстного меню выберите команду Sharing (Доступ). В диалоговом окне свойств отметьте переключатель Shared As (Общий доступ) и введите общее имя принтера. В больших организациях общее имя должно быть содержательным и полезным при определении местоположения печатающего устройства. Например, чтобы описать печатающее устройство, которое находится на двенадцатом этаже в северо-восточном крыле здания, можно назвать его TwelveNE.
4. Если принтер подключен к серверу Windows 2000, то после установки он сразу становится общим. Общим именем становятся первые 8 символов имени принтера, исключая пробелы. Все пробелы опускаются. Например, общим именем принтера HP DeskJet 890C будет HPDeskJet. Общее имя принтера можно изменить (см. п. 3).

Печатающее устройство не обнаружено

Если ОС не сможет обнаружить новое печатающее устройство, откроется диалоговое окно Add Printer Wizard (рис. 16-4). Щелкните кнопку Next. Вам придется вручную установить печатающее устройство.

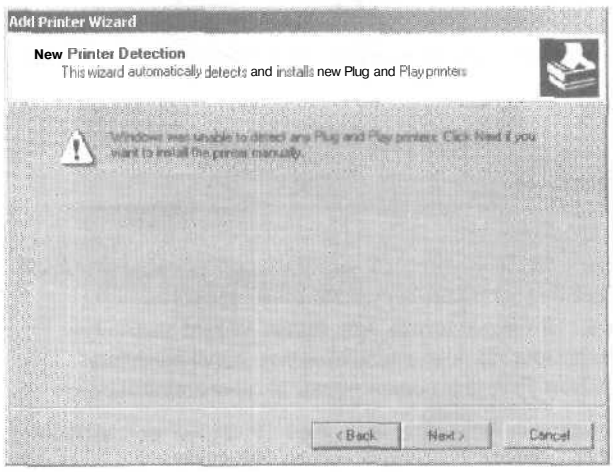


Рис. 16-4. Диалоговое окно Add Printer Wizard говорит о том, что ОС не смогла обнаружить новое печатающее устройство. Его придется устанавливать вручную.

1. В первую очередь нужно настроить порт принтера (рис. 16-5).
   - Если печатающее устройство подключено к серверу печати, выберите соответствующий порт LPT или COM. Вы можете также печатать в файл. В этом случае ОС будет запрашивать имя файла при каждой попытке печати. Щелкните кнопку Next и пропустите пи. 2-8.
   - Если печатающее устройство подключено к сети напрямую, щелкните Create A New Port (Создать новый порт) и отметьте переключатель Standard TCP/IP Port, Щелкните кнопку Next. Запустится мастер Add Standard TCP/IP Printer Port Wizard (Мастер добавления стандартного TCP/IP порта принтера).

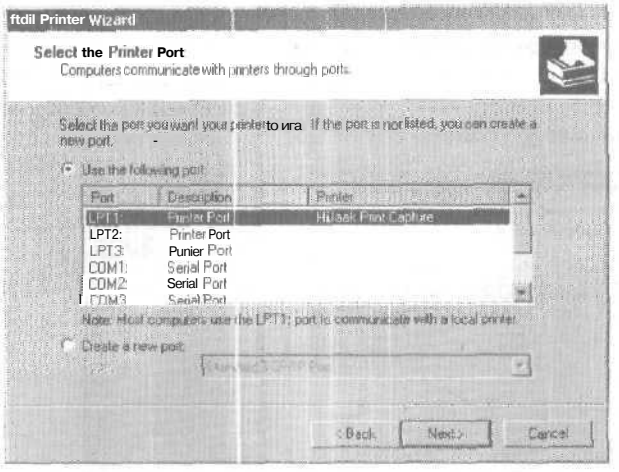


Рис. 16-5. В окне мастера Add Printer Wizard выберите порт для поиска принтера или отметьте переключатель Create A New Port для подключения сетевого принтера.

2. В окне мастера введите имя или IP-адрес печатающего устройства. Поле с именем порта заполнится автоматически. Например, если вы ввели IP-адрес 192.168.12.8, именем порта будет IP_192.168.12.8.

Совет Имя порта не имеет значения до тех пор, пока оно уникально в системе. Если вы настраиваете сервер печати, который будет поддерживать несколько принтеров, запишите их имена на карту принтеров.

3. Щелкните кнопку Next; мастер попытается обнаружить печатающее устройство. В случае неудачи убедитесь, что:
   - устройство включено и подксоединено к сети;
   - принтер настроен правильно;
   - IP-адрес и имя принтера в предыдущем окне указаны верно.
4. Если IP-адрес или имя принтера указаны неверно, щелкните кнопку Back (Назад) и заново введите информацию.
5. Если информация задана верно, нужно указать дополнительные параметры, идентифицирующие устройство. В области Device Type (Тип устройства) отметьте переключатель Standard или Custom. После этого в первом

случае выберите стандартный принтер, а во втором – щелкните кнопку Settings (Параметры), чтобы указать специфические параметры принтера, такие как протокол и состояние протокола SNMP.

6. Щелкните кнопку Next, а затем Finish, чтобы завершить настройку нового порта. Мастер Add Printer Wizard начнет устанавливать принтер.
7. В следующем окне мастера (рис. 16-6) укажите производителя и модель принтера. Это необходимо для того, чтобы Windows 2000 смогла подобрать нужный драйвер для печатающего устройства. Если производителя или модели печатающего устройства в списке нет, щелкните кнопку Have Disk (Установить с диска), чтобы установить новый драйвер.

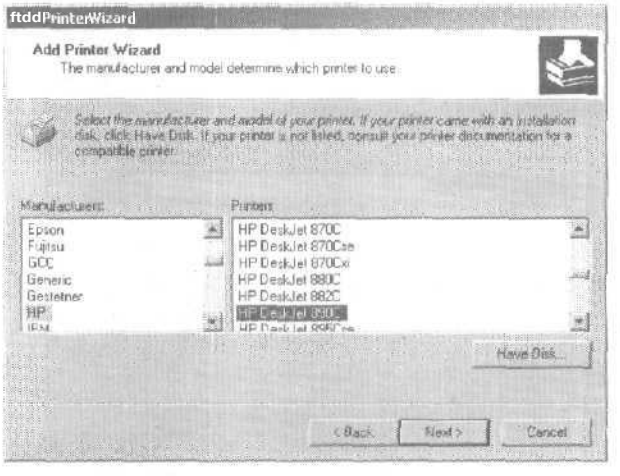


Рис. 16-6. Выбор изготовителя и модели принтера с помощью мастера Add Printer Wizard.

8. Щелкните кнопку Next. Если драйвер принтера уже установлен, ОС предложит заменить его или оставить неизменным. Щелкните кнопку Next.

Примечание Если у вас нет драйвера для данной модели принтера, можете выбрать драйвер, характерный для данного класса, либо драйвер похожего печатающего устройства. Подробности — в документации к печатающему устройству.

9. Укажите имя принтера. Это имя вы будете видеть в папке Printers (Принтеры) в Control Panel (Панель управления). При установке локального принтера вы можете сделать его принтером по умолчанию.
10. Укажите, должен ли принтер быть доступным для удаленных пользователей (рис. 16-7). Чтобы создать сетевой принтер и открыть доступ удаленным пользователям, отметьте переключатель Share *As* (Общий доступ) и введите общее имя принтера. В больших организациях общее имя должно быть содержательным и удобным при определении местоположения печатающего устройства. Например, чтобы описать печатающее устройство, которое находится на двенадцатом этаже в северо-восточном крыле здания, можно назвать его TwelveNE.

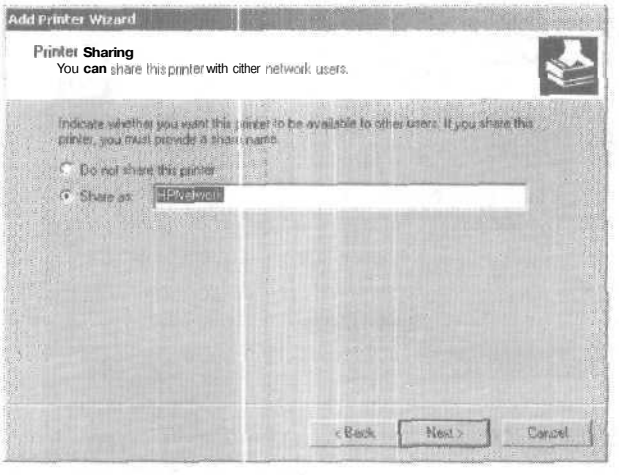


Рис. 16-7. Открытие доступа к сетевому принтеру и определение общего имени с помощью мастера.

Примечание Если к принтеру будут обращаться клиенты под управлением Windows 3.1 или MS-DOS, то его имя должно подчиняться правилу образования имен MS-DOS, например, вместо имени NORTH_PRINTER_FLOOR12 следует использовать NORTH12.PRT. О правиле образования имен MS-DOS см. главу 12.

11. При желании укажите комментарии и сведения о расположении. Эта информация поможет пользователям найти нужный принтер и определить его возможности.
12. Последнее окно мастера позволяет проверить правильность установки принтера, напечатав пробную страницу. Чтобы напечатать пробную страницу, отметьте переключатель Yes (Да). Щелкните кнопку Finish, чтобы завершить установку.

После установки принтера в папке Printers в Control Panel появится новый значок с его именем. В любой момент вы можете изменить свойства и состояние принтера. Подробнее об этом см. раздел «Настройка свойств принтера».

Совет Повторяя этот процесс, можно создать дополнительные принтеры для данного печатающего устройства. Вам нужно изменить лишь имя порта и общее имя принтера. Наличие нескольких принтеров у одного печатающего устройства позволяет по-разному настроить каждый из них и, значит, лучше приспособить к решению различных задач. Так, можно создать принтер с высоким приоритетом для печати неотложных заданий и принтер с низким приоритетом для заданий, которые могут подождать.

Установка локального печатающего устройства

Локальное печатающее устройство доступно только с того компьютера, к которому подключено. Установка печатающего устройства на локальном компьютере практически не отличается от его установки на сервере печати. Ключевое отличие в том, что локальный принтер не назначается общим. Поэтому, чтобы установить локальное печатающее устройство, сделайте, как рассказано в разделе «Установка печатающего устройства на локальном или удаленном сервере печати». Укажите, что принтер не является общим.

Примечание Локальный принтер легко сделать сетевым. Подробнее об этом см. раздел «Открытие и закрытие доступа к принтеру».

Соединение с сетевыми принтерами

После создания сетевого принтера удаленные пользователи могут легко создать соединение и приступить к печати. Вам

нужно настроить соединение с каждым пользователем, либо предоставить это им самим. Соединение с принтером в Windows 2000 создастся так.

1. Войдите в систему с правами пользователя. Дважды щелкните значок Printers (Принтеры) в Control Panel (Панель управления) или в меню Start\Settings (Пуск\Настройка) выберите команду Printers. Откроется папка Printers.
2. Дважды щелкните значок Add Printer (Установка принтера). Запустится мастер Add Printer Wizard (Установка принтера).
3. Отметьте переключатель Network Printer (Сетевой принтер) и щелкните кнопку Next (Далее).
4. В диалоговом окне Locate Your Printer (Поиск принтера) выберите метод поиска сетевого принтера (рис. 16-8):
   - **Find A Printer ID The Directory** позволяет найти принтер в службе Active Directory, Все общие принтеры в сети Windows 2000 автоматически попадают в Active Directory. Однако, они могут быть удалены оттуда.
   - **Type The Printer Name, Or Click** Next **To Browse For A Printer** позволяет найти общий принтер в сети так же, как в My Network Places (Мое сетевое окружение).

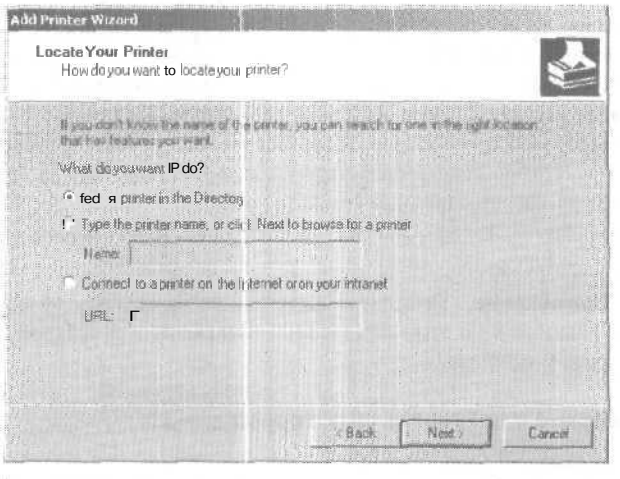


Рис. 16-8. Поиск принтера в сети или в Active Directory.

- Connect To A Printer On The Internet Or On Your Intranet позволяет ввести универсальный указатель ресурса (Uniform Resource Locator, URL) принтера в Интернет.

5. Щелкните OK.
6. Укажите, должен ли принтер использоваться по умолчанию в приложениях Windows, отметив переключатель Yes (Да) или No (Нет), и щелкните кнопку Next.
7. Щелкните кнопку Finish (Готово).

После соединения пользователи могут послать на сетевой принтер задания печати, выбрав его имя в приложении. Значок нового сетевого принтера появится в папке Printers. Этот значок позволяет настроить локальные параметры принтера. По умолчанию имя принтера имеет формат «Printer on Computer», например, HP DeskJet on Zeta.

Решение проблем буферизации

Б Windows 2000 буферизацией заданий печати управляет специальная служба. Если она не запущена, задания печати не могут буферизироваться. Состояние спулера печати (службы Print Spooler) позволяет проверить утилита Services (Службы) в Control Panel (Панель управления).

1. В меню Start\Programs\Administrative Tools выберите команду Computer Management (Управление компьютером), либо щелкните значок Computer Management в папке Administrative Tools.
2. Щелкните правой кнопкой узел Computer Management в дереве консоли и из контекстного меню выберите команду Connect To Another Computer (Подключиться к другому компьютеру). Выберите системы, службами которых вам нужно управлять.
3. Раскройте узел Services And Applications (Службы и приложения) и выберите узел Services (Службы).
4. Выберите службу Print Spooler (рис. 16-9). Б графе Status (Состояние) должно стоять «Started» («Запущена»). Иначе щелкните узел Print Spooler правой кнопкой и выберите команду Start. Параметр Startup Type (Тип запуска) должен быть равен «Automatic». В противном случае дважды щелкните узел Print Spooler и укажите нужное значение параметра.

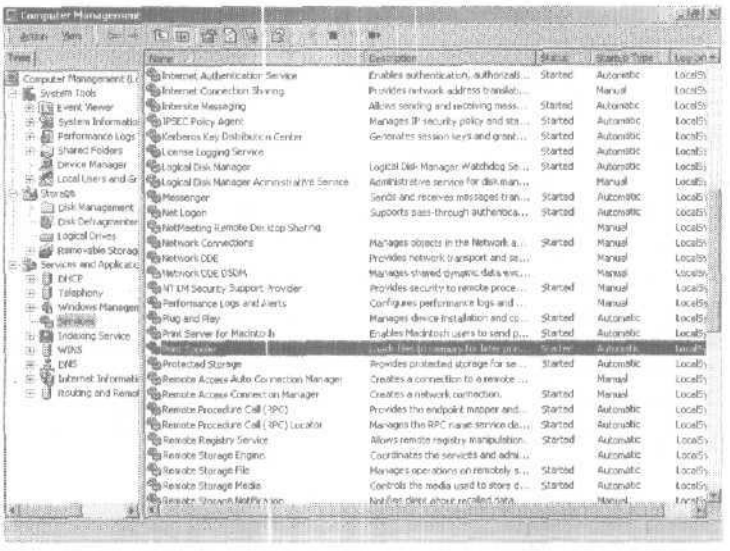


Рис. 16-9. Спулер печати управляет буферизацией заданий печати.

5. Если это не поможет, проверьте работу служб, от которых зависит спулер печати, например:
   - TCP/IP Print Server (Сервер печати TCP/IP);
   - Print Server for Macintosh (Сервер печати для Macintosh);
   - Print Server for Unix (Сервер печати для Unix).

Совет Иногда в работе спулера печати наблюдаются нарушения. Симптомы: зависший принтер, задания не посылаются на печатающее устройство, печатается мусор. Обычно остановка и повторный запуск спулера печати решают проблему.

О проблемах буферизации, связанных с разрешениями, см, раздел «Настройка разрешений доступа к принтерам».

Настройка свойств принтера

Свойства принтера назначаются в окне Properties (Свойства).

1. Откройте папку Printers (Принтеры) нужного сервера печати. Если вы обращаетесь к серверу печати локально,

в меню Start\Settings (Пуск\Настройка) выберите команду Printers, иначе откройте **My** Network Places (Мое сетевое окружение), войдите в домен, выберите нужный компьютер и дважды щелкните значок Printers.

2. Щелкните правой кнопкой значок нужного принтера и выберите команду Properties.
3. Откроется диалоговое окно свойств принтера (рис. 16-10).

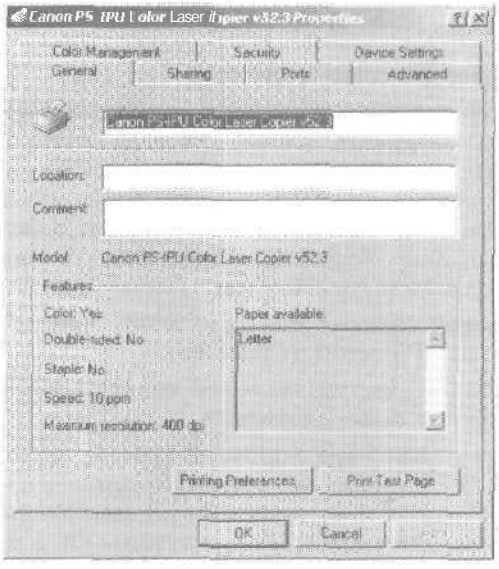


Рис. 16-10. Диалоговое окно свойств принтера

Комментарии и сведения о размещении указываются в полях Comment (Комментарий) и Location (Размещение) на вкладке General (Общие) диалогового окна свойств принтера.

Управление драйверами принтера

В домене Windows 2000 драйверы принтера можно настроить и обновить только на серверах печати. Драйверы не нужно обновлять на клиентских Windows-компьютерах, так как при необходимости они будут загружаться с сервера печати.

Обновление драйвера **принтера**

1. Откройте окно свойств принтера и выберите вкладку Advanced.

2. Список Driver (Драйвер) содержит драйверы, установленные в системе. Раскрывающийся список Driver содержит перечень известных драйверов.
3. Если в списке нет нужного или вы хотите установить новый драйвер, щелкните кнопку New Driver (Новый драйвер). Запустится мастер Add Printer Driver Wizard. Щелкните кнопку Next (Далее). Щелкните кнопку Have Disk, чтобы установить новый драйвер.
4. Щелкните кнопку Next, затем Finish.

Настройка драйверов для сетевых клиентов

Установив принтер или обновив драйвер, вы можете выбрать ОС, которые будут загружать драйвер с сервера печати. Это позволяет обновлять драйверы в одном месте. Иначе говоря, вместо установки нового драйвера на каждом компьютере вы устанавливаете его на сервере печати и даете возможность клиентам загрузить обновление. Чтобы клиенты смогли загрузить новый драйвер, сделайте так.

1. Щелкните правой кнопкой значок нужного принтера и выберите команду Properties (Свойства).
2. На вкладке Sharing (Доступ) щелкните кнопку Additional Drivers (Дополнительные драйверы).
3. Откроется диалоговое окно Additional Drivers, позволяющее выбрать ОС, которые могут загрузить драйвер принтера. При необходимости вставьте компакт-диск Windows 2000 или драйверами к принтеру для нужных ОС в привод CD-ROM. Компакт-диск Windows 2000 содержит драйверы для большинства ОС Windows и архитектур процессора.

Настройка страницы-разделителя и режима печати

Страницы-разделители в Windows 2000:

- печатаются в начале задания и облегчают поиск нужного документа;
- выполняют переключение между режимами печати PostScript и PCL (Printer Control Language).

Страница-разделитель для печатающего устройства настраивается так.

1. В диалоговом окне свойств нужного принтера выберите вкладку Advanced (Дополнительно) и щелкните кнопку Separator Page (Страница-разделитель).
2. В диалоговом окне Separator Page щелкните кнопку Browse (Обзор) и выберите одну страниц-разделителей:
   - **PCL.SEP** переключает печатающее устройство в режим PCL и печатает страницу-разделитель перед каждым документом;
   - **PSCRIPT.SEP** переключает печатающее устройство в режим PostScript, но не печатает страницу-разделитель;
   - **SYSPRINT.SEP** переключает печатающее устройство в режим PostScript и печатает страницу-разделитель перед каждым документом.

Чтобы отменить использование страницы-разделителя, откройте диалогоное окно Separator Page и удалите имя файла.

Изменение порта принтера

Порт принтера можно изменить в диалоговом окне свойств принтера. Открыв диалоговое окно свойств принтера, выберите вкладку Ports (Порты). Чтобы включить/отключить порт отметьте/снимите соответствующий ему флажок. Чтобы добавить порт, щелкните кнопку Add Port (Добавить порт) и выполните инструкции раздела «Установка печатающего устройства на локальном или удаленном сервере печати» для случая, когда ОС не может обнаружить печатающее устройство. Чтобы полностью удалить порт щелкните кнопку Delete Port (Удалить порт).

Настройка времени и приоритета заданий печати

Стандартное время и приоритет заданий печати можно настроить в диалоговом окне свойств принтера. Открыв диалоговое окно свойств принтера, выберите вкладку Advanced (рис. 16-11). Стандартное время и приоритет заданий печати настраиваются в полях, расположенных на этой вкладке.

Настройка времени доступа к принтеру

Принтеры доступны либо в любое время, либо только в определенные часы. Чтобы настроить время доступа к принтеру, выберите вкладку Advanced. Переключатель Always Available (Доступен всегда) открывает доступ к принтеру в

любое время, а переключатель Available From (Доступен с)— только в определенные часы.

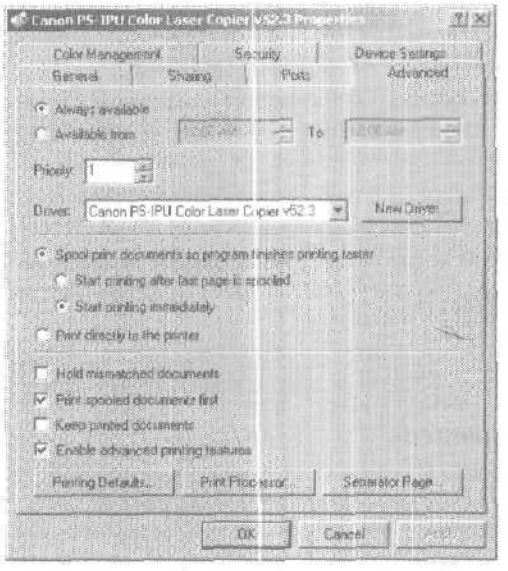


Рис. 16-11. Вкладка Advanced позволяет задать время и приоритет заданий печати.

Настройка приоритета принтера

Стандартный приоритет заданий печати задается в поле Priority (Приоритет), расположенном на вкладке Advanced. Задания печати всегда выполняются в порядке приоритета. Задания с высоким приоритетом печатаются первыми.

Настройка буферизации печати

При работе с печатающим устройством, подключенным к сети, обычно используют буферизацию файлов вместо их печати прямо на принтер. Буферизация позволяет управлять заданиями печати с помощью принтера.

Включение буферизации Буферизация **включается так** (рис. 16-11).

- Spool **Print Documents So Program Finishes** Printing **Faster.** Этот переключатель включает буферизацию заданий печати.

- Start **Printing After Last Page Is Spooled.** Отметьте этот переключатель, если хотите, чтобы документ полностью попал в буфер прежде, чем направиться на печать. Если почему-либо печать документа не завершится или будет отменена, задание печати не будет выполнено.
- Start Printing **Immediately.** Этот переключатель позволяет немедленно напечатать документ, если печатающее устройство не занято. Используйте его, если нужно напечатать документ или вернуть управление пользователю максимально быстро,

Другие параметры буферизации Флажок Print Directly To The Printer (Печатать прямо на принтер) позволяет выключить буферизацию. Остальные флажки служат для настройки параметров буферизации (рис. 16-11).

- Hold **Mismatched Documents.** Если отмечен этот флажок, спулер будет задерживать задания печати, которые не соответствуют параметрам печатающего устройства. Этот флажок удобен при частом изменении форматов печати или настроек лотка.
- Print Spooled **Documents First.** Если отмечен этот флажок, задание, прошедшее буферизацию, будет печататься перед заданиями, находящимися в процессе буферизации, независимо от их приоритета.
- Keep **Printed Documents.** Обычно документы удаляются из очереди после печати. Этот флажок позволяет сохранить копию документа в принтере. Как правило, он используется при печати трудновосстанавливаемых файлов. В этом случае сохраняется напечатать документ, не прибегая к его восстановлению. Подробнее об этом в разделе «Приостановка, возобновление и повтор печати отдельных документов».
- **Enable Advanced Printing** Features. Флажок разрешает задать дополнительные параметры печати (если таковые имеются), например, Page Order (Порядок страниц) и Pages Per Sheet (Страниц на каждом листе). Если при использовании дополнительных параметров вы заметите проблемы с совместимостью, снимите этот флажок.

Открытие и закрытие доступа к принтеру

Для настройки доступа к принтеру служит диалоговое окно свойств принтера. Чтобы открыть его, щелкните правой кноп-

кой значок нужного принтера и из контекстного меню выберите команду Sharing (Доступ). Диалоговое окно свойств принтера позволяет изменить общее имя принтера, а также открыть или закрыть доступ к принтеру.

- Открытие доступа к локальному принтеру (т. е. его преобразование в сетевой принтер). Чтобы открыть доступ к принтеру, отметьте переключатель Share As (Общий доступ) и укажите имя общего ресурса. Если к принтеру обращаются клиенты под управлением Windows 3.1 или MS-DOS, общее имя должно удовлетворять формату 8.3, например, SOUTHEAS.PRT вместо SOUTHEAST_PRINTER. Щелкните OK.
- **Изменение общего имени принтера.** Чтобы изменить общее имя принтера, просто введите его в поле Share As и щелкните OK.
- **Закрытие доступа к принтеру.** Чтобы закрыть доступ к общему принтеру, щелкните Not Shared (Локальный), а затем — OK.

Настройка разрешений доступа к принтерам

Так как сетевые принтеры являются общими ресурсами, доступ к ним можно ограничить, используя разрешения. Для настройки разрешений доступа служит диалоговое окно свойств принтера. Открыв окно свойств принтера, выберите вкладку Security (Безопасность) и щелкните кнопку Permissions (Разрешения). Откроется диалоговое окно Printer Permissions.

ОС Windows 2000 поддерживает три разрешения доступа к принтерам: Print, Manage Documents и Manage Printers, которые можно предоставлять и блокировать (табл. 16-2).

При создании каждому принтеру назначаются стандартные разрешения доступа:

- группам Administrators, Print Operators и Server Operators — полный контроль над принтерами. Сюда входит администрирование принтера и его заданий печати;
- создателю и владельцу — право управления своим документом, что позволяет лицу, пославшему задание печати, изменить параметры и удалить документ;
- группе Everyone — право печати, что делает принтер доступным для всех пользователей сети.

Табл. 16-2. Разрешения доступа к принтерам в Windows 2000.

Разрешение	Print (Печать)	Manage Documents (Управление документами)	Manage Printers (Управление принтерами)
Печать документа	+	+	+
Приостановка, возобновление, повтор и отмена печати документа, отосланного непосредственно пользователем	+	+	+
Подключение к принтеру	+	+	+
Управление параметрами заданий печати		+	+
Приостановка, повтор и удаление заданий печати		+	+
Совместное использование принтера			+
Изменение свойств принтера			+
Изменение разрешений принтера			+
Удаление принтера			+

Как и остальные наборы разрешений, базовые разрешения для принтеров представляют собой скомбинированные в логические группы специальные разрешения. Ниже перечислены специальные разрешения, используемые для создания базовых разрешений для принтеров (табл. 16-3). Щелкнув кнопку Advanced (Дополнительно), вы можете назначить эти специальные разрешения индивидуально.

Табл. 16-3. Специальные разрешения доступа к принтерам.

Разрешение	**Print (Печать)**	**Manage Documents (Управление документами)**	**Manage Printers (Управление принтерами)**
Печать	+		+
Управление документами		+	
Управление принтерами			+
Просмотр разрешений	+	+	+
Изменение разрешений		+	+
Получение прав владельца принтера		+	+

Аудит заданий печати

Windows 2000 поддерживает аудит большинства операций с принтером. Аудит операций с принтером настраивается так.

1. Откройте диалоговое окно свойств принтера, выберите вкладку Security и щелкните кнопку Advanced. Откроется диалоговое окно Access Control Settings.

Примечание По умолчанию операции с принтером не подлежат аудиту. Чтобы разрешить аудит, нужно настроить соответствующую групповую политику.

2. Выберите вкладку Auditing (Аудит) и, используя кнопки Add (Добавить) и Remove (Удалить), сформируйте список пользователей и групп, действия которых должны подлежать аудиту.
3. С помощью флажков под заголовками Successful (Успешные) и Failed (Неудачные) выберите события, которые должны подлежать аудиту.
4. Щелкните OK.

Установка стандартных параметров документа

Стандартные параметры документа применяются при печати из программ, не являющихся приложениями Windows, например, командной строки MS-DOS. Стандартные параметры документа устанавливаются так.

1. Откройте папку Printers (Принтеры) и дважды щелкните значок нужного принтера.
2. В окне управления печатью документов, в меню Printer (Принтер) выберите команду Printing Preferences.
3. Установите стандартные параметры документа на вкладках Layout и Paper/Quality.

Настройка свойств сервера печати

Диалоговое окно Print Server Properties (Свойства сервера печати) позволяет управлять глобальными параметрами серверов печати. Оно открывается так.

1. Откройте папку Printers (Принтеры) нужного сервера печати. Если вы обращаетесь к серверу печати локально, в меню Start\Settings (Пуск\Настройка) выберите команду

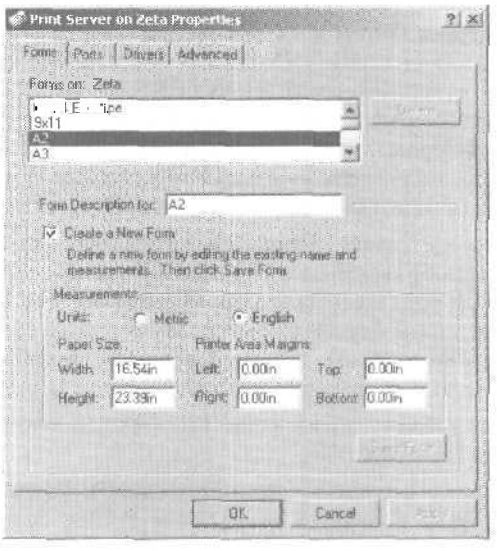
Printers, в противном случае откройте My Network Places (Мое сетевое окружение), войдите в домен, выберите нужный компьютер и дважды щелкните значок Printers.

2. В окне Printers (Принтеры) откройте меню File (Файл) и выберите команду Server Properties (Свойства сервера) либо щелкните свободное место правой кнопкой и из контекстного меню выберите команду Server Properties.

Просмотр и создание форматов печати

Форматы печати определяют стандартные размеры бумаги, границ и степень прозрачности. Просмотреть текущие параметры формата печати можно так.

1. Откройте диалоговое окно свойств сервера печати и выберите вкладку Forms (Форматы) (рис. 16-12).



Рис, 16-12. Просмотр форматов печати в диалоговом окне свойств сервера печати.

2. Выберите нужный формат печати о списке Forms On.
3. Параметры формата показаны в области Measurements (Размеры). Стандартные системные форматы ни изменить, ни удалить нельзя.

Новая форма создается так.

1. В диалоговом окне свойств сервера печати выберите вкладку Forms.
2. В списке Forms On выберите базовый формат печати.
3. Отметьте флажок Create A New Form (Создать новый формат).
4. В поле Form Description For введите новое имя формата.
5. В области Measurements настройте границы и размер бумаги.
6. Щелкните кнопку Save Form (Сохранить формат), чтобы сохранить формат.

Изменение местоположения папки Spool и разрешение печати в NTFS

Папка Spool содержит копии всех документов, которые находятся в очереди печати. По умолчанию она расположена в *%SystemRoot%*\system32\spool\PRINTERS. В файловой системе NTFS (Windows NT File System) все пользователи, работающие с принтером, должны иметь разрешение Change для этого каталога, иначе они не смогут печатать документы. Разрешение для этого каталога можно проверить так.

1. Откройте папку Printers (Принтеры) нужного сервера печати. Если вы обращаетесь к серверу печати локально, в меню Start\Settings (Пуск\Настройка) выберите команду Printers', в противном случае откройте My Network Places (Мое сетевое окружение), войдите в домен, выберите нужный компьютер и дважды щелкните значок Printers.
2. В окне Printers (Принтеры) в меню File (Файл) выберите команду Server Properties.
3. Выберите вкладку Advanced (Дополнительно). Расположение папки Spool указано в поле Spool Folder. Запомните его.
4. Щелкните правой кнопкой папку Spool в Microsoft Windows 2000 Explorer и выберите Properties (Свойства).
5. В окне свойств выберите вкладку Security (Безопасность). Проверьте правильность разрешений.

Управление печатью большого объема

В больших корпорациях принтеры ежедневно печатают сотни и тысячи документов. Такая нагрузка требует высокой производительности от серверов печати. При недостатке производительности могут возникнуть задержки печати, разрушение документов и другие проблемы. Ниже перечислены способы повышения производительности серверов печати.

- Подключайте принтеры к сети напрямую, а не через последовательный, параллельный или инфракрасный порты. При таком способе подключения требуется меньше системных ресурсов (процессорного времени).
- Выделите отдельный сервер для задач печати. Если сервер печати занят решением других задач, он теряет способность к быстрому реагированию на запросы печати и управления. Чтобы увеличить способность к реагированию, распределите другие сетевые задачи по другим серверам.
- Переместите папку Spool (по умолчанию она хранится там же, где и ОС) на отдельный жесткий диск, предназначенный для печати. Производительность операций ввода-вывода можно повысить, используя диск с отдельным контроллером.

Регистрация событий, связанных с работой принтера

Для настройки регистрации событий, связанных с работой принтера служит окно свойств сервера печати. Отрыв его, выберите вкладку Advanced (Дополнительно) и с помощью флажков выберите события, которые нужно регистрировать.

Уведомление о завершении задания печати

Серверы печати могут уведомлять пользователей о завершении печати документа. По умолчанию эта возможность выключена, так как иногда она раздражает. Чтобы создать/удалить уведомление, откройте диалоговое окно свойств сервера печати, выберите вкладку Advanced и отметьте/снимите флажок Notify When Remote Documents Are Printed. Кроме того, можно отметить/снять флажок Notify Computer, Not User, When Remote Documents Are Printed.

Управление заданиями печати локальных и удаленных принтеров

Для управления принтерами и заданиями печати служит окно Print Management, которое открывается так.

1. Откройте Control Panel (Панель управления) и дважды щелкните значок Printers (Принтеры), либо в меню Start\ Settings (Пуск\Настройка) выберите команду Printers.
2. Дважды щелкните значок нужного принтера.

Окно управления печатью документов для удаленного принтера открывается так.

1. Запустите Windows Explorer и выберите нужный сервер печати в My Network Places (Мое сетевое окружение).
2. Откройте папку Printers и дважды щелкните значок нужного принтера.

Использование окна управления печатью документов

Окно управления печатью документов позволяет управлять принтерами и заданиями печати (рис. 16-13), В нем представлена информация о документах, которые находятся в очереди печати, а именно:

- **Document** Name (Документ) — имя файла документа, которое может включать имя приложения, отправившего его на печать;
- **Status** (Состояние) — состояние задания печати (состояние документа или принтера). Состояния документа: Printing (Печать), Spooling (Буферизация), Paused (Приостановка), Deleting (Удаление) и Restarting (Повторная печать); состоянию документа может предшествовать состояние принтера, например, Printer Off-Line (Принтер не готов к работе);
- **Owner** (Владелец) — владелец документа;
- **Pages** (Число страниц) — количество страниц в документе;
- **Size** (Размер) — размер документа в кило- или мегабайтах;
- **Submitted** (Постановка в очередь) — дата и время отправки документа на печать;
- **Port** (Порт) — порг, используемый при печати, например, LPT1, COM3 или File.

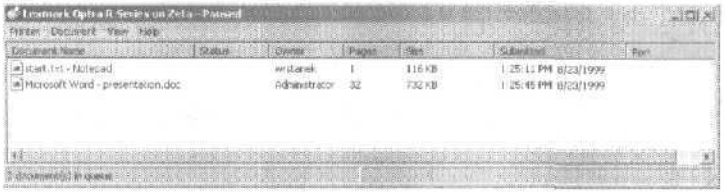


Рис. 16-13. Управление принтерами и заданиями печати из окна управления печатью документов.

Приостановка принтера и возобновление печати

Чтобы приостановить работу принтера, раскройте меню Printer (Принтер) и выберите команду Pause Printing (Приостановить печать); появится флажок, который говорит о том, что работа принтера приостановлена. Принтер закончит выполнение текущего задания печати и приостановит печать оставшихся документов.

Чтобы возобновить работу принтера, снова дайте команду Pause Printing. Галочка рядом с ней должна исчезнуть.

Очистка очереди печати

Окно управления печатью документов позволяет очистить очередь печати. Для этого в меню Printer (Принтер) выберите команду Cancel All Documents (Очистить очередь печати).

Приостановка, возобновление и повтор печати отдельных документов

Состояние отдельных документов настраивается в окне управления печатью документов.

1. Выберите нужный документ в окне управления печатью документов.
2. В меню Document (Документ) выберите одну из следующих команд:
   - Pause приостанавливает печать документа и уступает очередь печати другим документам;
   - Resume возобновляет печать документа с того места, где она была приостановлена;
   - Restart печатает документ с начала.

Удаление документа и отмена задания печати

Вы можете удалить документ из очереди печати или отменить задание печати.

1. Выберите нужный документ в окне управления печатью документов.
2. В меню Document (Документ) выберите команду Cancel (Отменить) или нажмите клавишу DEL.

Примечание Большинство печатающих устройств кэшируют документы во внутреннем буфере, поэтому при отмене текущего задания печати печать документа может завершиться не сразу.

Просмотр свойств документа в очереди печати

Вы можете просмотреть свойства документа (источник страницы, ориентация, размер), находящегося в очереди печати.

- Выберите нужный документ в окне управления печатью документов. В меню Document (Документ) выберите команду Properties (Свойства).
- Дважды щелкните нужный документ в окне управления печатью документов.

Настройка приоритета отдельных документов

Приоритет документа определяет очередность печати. Документы с высоким приоритетом печатаются первыми. Приоритет отдельных документов настраивается так.

1. Выберите нужный документ в окне управления печатью документов и в меню Document (Документ) — команду Properties (Свойства).
2. В окне свойств принтера выберите вкладку General (Общие), в поле Priority (Приоритет) укажите приоритет документа: минимальный — 1, максимальный — 99.

Настройка времени печати отдельных документов

Если организация ежедневно печатает большое количество документов, ей может понадобиться составить расписание печати. Например, можно сделать так, чтобы большие задания печати с низким приоритетом выполнялись ночью. Время печати документа настраивается так.

1. Выберите нужный документ в окне управления печатью документов и в меню Document — команду Properties.
2. В окне свойств принтера выберите вкладку General (Общие), отметьте переключатель Only From (Только с) и задайте временной интервал, например, с полуночи до пяти часов утра. Теперь выбранный документ может быть напечатан только в указанный промежуток времени.

Глава 17

Клиенты и серверы DHCP

Протокол динамической конфигурации узла (Dynamic Host Configuration Protocol, DHCP) разработан для облегчения администрирования доменов службы каталогов Active Directory. DHCP служит для динамической конфигурации протокола TCP/IP на сетевых клиентах. При этом не только экономится время на настройку системы, но и создается централизованный механизм изменения конфигурации. Для запуска в сети DHCP нужно настроить DHCP-ссрвср, предоставляющий сведения о сетевой конфигурации.

Понятие DHCP

DHCP — средство централизованного управления выделением IP-адресов и не только. Если в сети есть DHCP-сервер, вы можете присвоить динамический IP-адрес любому сетевому адаптеру компьютера. Установив DHCP-сервер, вы поручаете ему выдавать основную информацию, нужную для работы сети TCP/IP: IP-адрес, маску подсети, сведения о маршрутизаторе по умолчанию, первичном и вторичном DNS- и WINS-серверах, а также имя домена DNS.

Клиент DHCP и IP-адрес

Компьютер, использующий динамический адрес, называют *клиентом DHCP*. При загрузке компьютера DHCP-клисит запрашивает IP-адрес из пула адресов, выделенных данному DHCP-серверу, и использует адрес определенное время, называемое *сроком аренды*. Спустя примерно половину этого срока клиент пытается возобновить его. Если клиент не может обновить аренду, он будет пытаться сделать это снова до окончания срока аренды. Если эти попытки не принесут успеха, клиент будет пытаться обратиться к другому DHCP-серверу. Невозобновленный IP-адрес возвращается в пул адресов. Если клиент связался с сервером, но текущий

IP-адрес не может быть возобновлен, DHCP-сервер присваивает клиенту новый IP-адрес.

DHCP-сервер обычно не влияет на процедуру загрузки или входа в сеть. Загрузка клиентов и регистрация пользователей возможна даже при нефункционирующем сервере DHCP. При загрузке клиент пытается найти сервер. Если это удалось, клиент получает нужную конфигурационную информацию от сервера. Если DHCP-ссрвер недоступен, а срок аренды клиента еще не истек, клиент пытается опросить стандартный шлюз, указанный при получении аренды. В случае успеха клиент считает, что, вероятно, находится в той же сети, в какой находился при получении аренды, и продолжит пользоваться арендой. Неудавшийся опрос означает, что клиент, возможно, находиться к другой сети. Тогда применяется автоконфигурация IP; ее также использует клиент, если сервер DHCP недоступен, а срок аренды истек.

Автоконфигурация IP работает следующим образом.

1. Компьютер клиента выбирает IP-адрес из зарезервированной Microsoft подсети класса B — 169.254.0.0, маска подсети 255.255.0.0. Прежде чем задействовать IP-адрес, клиент проводит проверку по протоколу разрешения адресов (Address Resolution Protocol, ARP), чтобы убедиться, что выбранный IP-адрес не используется другим клиентом.
2. Если IP-адрес уже занят, клиент повторяет п. 1. пробуя до 10 IP-адресов, после чего сообщает об ошибке.

Примечание Если клиент отключен от сети, проверка ARP всегда будет успешной, тогда используется первый выбранный IP-адрес.

3. Если IP-адрес свободен, клиент настраивает сетевой интерфейс, используя этот адрес. Затем клиент пытается связаться с сервером DHCP, отправляя в сеть широковещательные запросы каждые 5 минут. Установив связь с сервером, клиент получает аренду и перенастраивает сетевой интерфейс.

Проверка назначения IP-адреса

Узнать выданный IP-адрес и другие сведения о конфигурации позволяет утилита IPCONFIG. Чтобы получить информацию обо всех сетевых адаптерах компьютера, наберите в командной строке **IPCONFIG** /ALL. Если IP-адрес был на-

значен автоматически вы увидите строку Autoconfiguration IP Address. В этом примере автоматически назначен адрес 169.254.98.59:

```
Windows 2000 IP Configuration
    Host Name . . . . . : DELTA
    Primary DNS Suffix . . . . . : microsoft.com
    Node Type . . . . . : Hybrid
    IP flouting Enabled . . . . . : No
    WINS Proxy Enabled . . . . . : No
    DNS Suffix Search List . . . . . : microsoft.com
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . . . :
    Description . . . . . : NDC ND5300 PnP
     Ethernet Adapter
    Physical Address . . . . . :03-82-C6-F8-EA-69
    DHCP Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Autoconfiguration IP Address . . . :169.254.98.59
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :
    DNS Servers . . . . . :
```

Понятие областей

Области — это пулы IP-адресов, присваиваемых клиентам в процессе аренды и резервирования. Резервирование отличается от аренды тем, что при этом компьютеру присваивается конкретный IP-адрес, пока вы не снимите резервирование. Так можно присвоить «постоянные» адреса ограниченному кругу клиентов DHCP.

Области создаются для выделения диапазонов IP-адресов, доступных клиентам DHCP. Например, вы можете выделить диапазон IP-адресов 192.168.12.2 - 192.168.12.250 для основной области предприятия. В областях можно использовать открытые или частные IP-адреса:

- сеть класса A: 1.0.0.0 - 126.255.255.255;
- сеть класса B: 128.0.0.0 - 191.255.255.255;
- сеть класса C: 192.0.0.0 - 223.255.255.255;
- сеть класса D: 224.0.0.0 - 239.255.255.255.

Примечание IP-адрес 127.0.0.1 используется в качестве локальной петли возврата.

Один сервер DHCP может управлять несколькими областями следующих типов.

- **Обычные области** служат для присвоения пулов адресов сетям класса A, B и C.
- **Многоадресные области** позволяют присвоить пул адресов сетям класса D. Компьютеры используют групповые IP-адреса как вторичные в дополнение к стандартному IP-адресу в сетях класса A, B или C.
- **Суперобласти** — контейнеры, которые содержат другие области и упрощают управление большим количеством областей.

Совет Хотя вы можете создавать области в разных сегментах сети, рекомендуется, чтобы эти сегменты находились в сети одного класса. Не забудьте настроить трансляцию DHCP для передачи широковещательных запросов между сегментами сети. Вы можете настроить агенты ретрансляции средствами службы маршрутизации и удаленного доступа Windows 2000 (Routing and Remote Access Service, RRAS) и службы агента ретрансляции DHCP из состава Windows NT Server 4.0. Кроме того, в качестве агентов ретрансляции можно использовать некоторые маршрутизаторы.

Установка сервера DHCP

Динамическое выделение IP-адресов возможно, только если в сети имеется DHCP- сервер. Компоненты DHCP устанавливаются при помощи мастера установки компонентов Windows, после чего из консоли DHCP запускается и авторизуется сервер домена. Предоставлять клиентам динамические IP-адреса могут только авторизованные серверы DHCP.

Установка компонентов DHCP

Чтобы сервер Windows 2000 мог работать в качестве DHCP-сервера, сделайте так.

1. Щелкните Start (Пуск), Settings (Настройка); затем Control Panel (Панель управления).
2. На панели управления дважды щелкните Add/Remove Programs (Установка и удаление программ), затем выберите Add/Remove Windows Components (Добавление и удаление компонентов Windows). Окно изменится.

3. Среди компонентов выберите Networking Services (Сетевые службы) и щелкните Details (Состав).
4. В субкомпонентах сетевых служи отметьте флажком Dynamic Host Configuration Protocol (DHCP).
5. Щелкните OK, затем — Next. В ответ на приглашение укажите путь к файлам дистрибутива Windows 2000 и щелкните Continue (Продолжить).

С этого момента служба Microsoft DHCP будет автоматически запускаться при каждой загрузке сервера (или запустите ее вручную — см. раздел «Запуск и остановка сервера DHCP»).

Запуск и использование консоли DHCP

После установки сервера DHCP настройка и управление динамической IP-адресацией осуществляется из консоли DHCP (рис. 17-1). Чтобы запустить консоль DHCP, раскройте меню Start\Programs\Administrative Tools и выберите DHCP. В главном окне консоли DHCP две панели. Слева перечислены серверы DHCP по порядку их IP-адресов, а также локальные компьютеры (если окно открыто на сервере DHCP). Двойным щелчком можно открыть каждый объект,

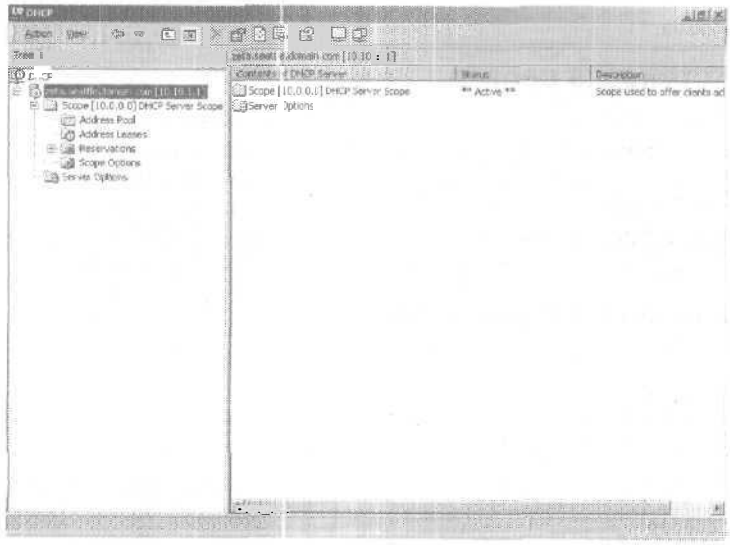


Рис. 17-1. Консоль DHCP позволяет создавать и изменять конфигурацию сервера DHCP.

чтобы просмотреть области и настроить DHCP-серверы. Справа — подробные сведения о выбранном объекте.

Значки серверов и узлов областей отображают их текущее состояние. Для серверов значки могут быть такими:

- зеленая стрелка-вверх — служба DHCP запущена, сервер активен;
- красная буква X — у консоли нет доступа к серверу: служба DHCP остановлена либо сервер недоступен;
- красная стрелка-вниз — сервер DHCP неавторизован;
- синий значок предупреждения — состояние сервера изменилось, или появилось предупреждение об этом.

Значки областей могут выглядеть так:

- красная стрелка-вниз — область неактивна;
- синий значок предупреждения — состояние области изменилось, или появилось предупреждение об этом.

Соединение с удаленными серверами DHCP

Открыв консоль DHCP, вы напрямую подключитесь к локальному серверу, но не увидите удаленных серверов DHCP. Вы можете подключиться к удаленным серверам.

1. Щелкните правой кнопкой корень консоли DHCP и выберите Add Server (Добавить сервер). Появится диалоговое окно (рис. 17-2).

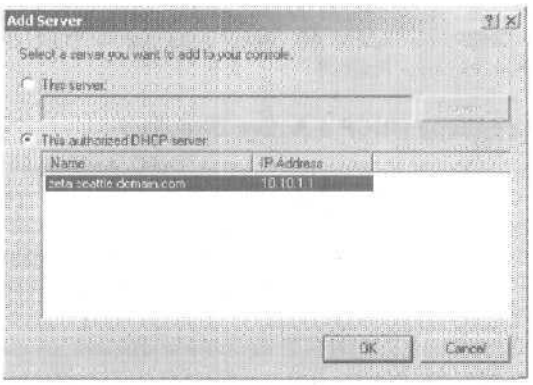


Рис. 17-2. Если вашего сервера DHCP нет в консоли, добавьте его.

2. Выберите This Server (Этот сервер), затем введите IP-адрес или имя компьютера — сервера DHCP, которым хотите управлять. Если хотите управлять только авторизованными серверами DHCP, выберите This Authorized DHCP Server (Этот авторизованный DHCP-сервер) и щелкните сервер, который хотите добавить. Помните, что можете управлять только серверами в доверенных доменах.
3. Щелкните **OK. В дереве** консоли **появится новый элемент - сервер DHCP.**

Примечание Управлять локальными и удаленными DHCP-серверами можно из консоли Computer Management. Запустите ее и подключитесь к серверу, которым хотите управлять. Затем раскройте Services And Applications (Службы и приложения) и выберите DHCP .

Запуск и остановка сервера DHCP

Серверами DHCP управляют с помощью службы DHCP Server. Как и любую другую, вы можете ее запустить, отключить, приостановить и возобновить из узла Services консоли Computer Management или из командной строки. Кроме того, службой DHCP можно управлять из консоли DHCP. Щелкните в ней правой кнопкой сервер, которым хотите управлять, выберите All Tasks, а затем — Start, Stop, Pause, Resume или Restart.

Примечание В Computer Management щелкните правой кнопкой DHCP, выберите All Tasks, а затем — Start, Stop, Pause, Resume или Restart.

Авторизация сервера DHCP в Active Directory

Перед использованием в домене сервера DHCP вы должны авторизовать его в службе каталогов Active Directory. Авторизация означает, что сервер правомочен выдавать динамические TP-адреса в домене. Windows 2000 требует авторизации, чтобы предотвратить обслуживание клиентов домена чужими серверами.

Для авторизации в консоли DHCP щелкните правой кнопкой сервер и выберите Authorize, а для отмены авторизации - Unauthorize.

Примечание В Computer Management щелкните правой кнопкой DHCP и выберите Authorize, для отмены авторизации — Unauthorize.

Настройка серверов DHCP

При установке нового сервера DHCP оптимальные параметры сетевого окружения задаются автоматически. Обычно их не меняют, пока не приходится решать проблемы производительности или вводить/удалять дополнительные параметры. Параметры сервера DHCP настраиваются в окне свойств (рис. 17-3). Вы можете вызвать его из консоли DHCP, щелкнув правой кнопкой нужный сервер и выбрав Properties (в Computer Management щелкните правой кнопкой DHCP).

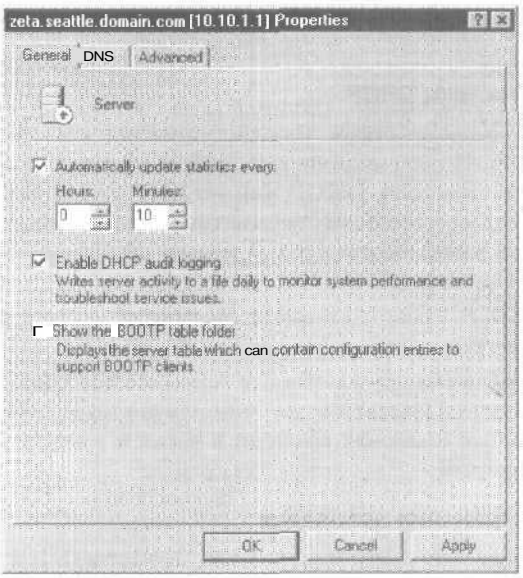


Рис. 17-3. Управление статистикой, аудитом, интеграцией DNS и другими свойствами из окна DHCP Server Properties.

Привязка многоадресного сервера DHCP к конкретному IP-адресу

Сервер с несколькими сетевыми адаптерами имеет несколько сетевых подключений и может предоставлять службу DHCP по любому из них. Но вам может потребоваться, что-

бы сервер DHCP обслуживал не все доступные соединения. Например, если сервер подключен к сетям 10 и 100 Мб/с, вы можете захотеть, чтобы весь DHCP-трафик проходил через соединение 100 Мб/с.

Для привязки DHCP к конкретному сетевому соединению сделайте так.

1. В консоли DHCP правой кнопкой щелкните нужный сервер и выберите Properties.
2. Щелкните Bindings (Привязки) на вкладке Advanced окна свойств.
3. Появится список сетевых подключений, доступных для сервера DHCP. Если вы хотите использовать службу сервера DHCP для соединения с клиентом, отметьте это соединение флажком, иначе снимите соответствующий флажок.

Обновление статистики DHCP

Консоль DHCP показывает статистику доступности и использования IP-адресов. По умолчанию статистика обновляется только при запуске консоли DHCP или по щелчку кнопки Refresh (Обновить) на панели инструментов. Если вы регулярно обращаетесь к статистике DHCP, можно настроить ее автоматическое обновление.

1. В консоли DHCP правой кнопкой щелкните сервер и выберите Properties.
2. На вкладке General (Общие) выберите Automatically Update Statistics Every (Автоматически обновлять статистику каждые) и введите интервал времени в часах и минутах. Затем щелкните OK.

Аудит DHCP и устранение неполадок

Windows 2000 изначально настроена на аудит процесса DHCP. При этом в журнале фиксируются запросы и процессы DHCP.

Понятие аудита DHCP

Для устранения неполадок DHCP можно использовать журнал аудита. По умолчанию он находится *в* папке *%SystemRoot%*\system32\DHCP — там хранятся отдельные файлы для каждого дня недели. Файл журнала для понедельника называется DhcpSrvLog.Mon, для вторника — DhcpSrvLog.Tue и т. д.

При запуске сервера DHCP или наступлении нового дня в файл журнала записывается сообщение-заголовок. В нем резюмированы события DHCP и их значение. При запуске и остановке службы DHCP файл журнала не обязательно очищается. Данные журнала обнуляются, только если запись в журнал не производилась последние 24 часа. Вам не нужно следить за использованием дискового пространства сервером DHCP — по умолчанию сервер делает это сам.

Разрешение и запрет аудита DHCP

1. В консоли DHCP правой кнопкой щелкните сервер и выберите Properties.
2. На вкладке General выберите Enable DHCP Audit Logging (Вести журнал аудита DHCP). Щелкните OK.

Размещение журналов DHCP

По умолчанию журналы DHCP хранятся в папке *%SystemRoot%*\system32\DHCP, но вы можете изменить их расположение.

1. В консоли DHCP правой кнопкой щелкните нужный сервер и выберите Properties.
2. На вкладке Advanced в поле Audit Log File Path (Путь к файлу журнала аудита) показан путь к размещению файлов журнала. Введите новый путь к файлам или щелкните Browse (Обзор), чтобы выбрать новую папку.
3. Щелкните OK. Windows 2000 потребует перезапустить службу сервера DHCP. В ответ на предложение подтвердить перезапуск щелкните Yes. Служба будет остановлена и запущена заново.

Изменение параметров журнала

В сервер DHCP встроен мониторинг использования дискового пространства. По умолчанию максимальный размер всех файлов журнала сервера DHCP — 7 Мб, причем каждый отдельный файл может занимать не более 1/7 этого объема. Если лимит в 7 Мб превышается, либо отдельный файл журнала выходит за пределы отведенного ему места, запись журнала DHCP прекращается, пока не будут очищены файлы журнала, либо место освобождается иначе. Обычно это происходит в начале дня, когда сервер очищает файл журнала за прошлую неделю.

Параметры реестра, управляющие журналом и другими параметрами DHCP, расположены в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters. Записью журнала управляют следующие параметры реестра:

- **DhcpLogFilesMaxSize** задает максимальный размер всех файлов журнала (по умолчанию 7 Мб);
- **DhcpLogDiskSpaceCheckInterval** определяет, как часто будет проверяться использование дискового пространства (по умолчанию каждые 50 минут);
- DhcpLogMinSpaceOnDisk устанавливает пороговое значение свободного места па диске; если свободного места на диске меньше, запись журнала временно прекращается (по умолчанию 20 Мб).

Интеграция DHCP и DNS

DNS используется для разрешения имен компьютеров в доменах Active Directory и в Интернете. Протокол обновления DNS избавляет вас регистрации клиентов DHCP в DNS вручную. Протокол позволяет клиенту и серверу DHCP при необходимости зарегистрировать записи прямого и обратного просмотра в DNS. В стандартной конфигурации DHCP клиенты под управлением Windows 2000 автоматически обновляют свои записи в DNS после аренды IP-адреса. Сервер DHCP обновляет записи о клиентах с более ранними версиями Windows после предоставления аренды.

Совет Серверы DNS на базе Windows NT 4.0 не поддерживают протокол динамического обновления, поэтому их записи не будут автоматически обновляться. Есть способ обойти это ограничение: разрешить поиск WINS для клиентов DHCP, использующих NetBIOS. Тогда клиенты смогут найти другие компьютеры средствами WINS. Но лучше обновить старые серверы DNS до Windows 2000.

Посмотреть и изменить параметры интеграции с DNS можно так.

1. В консоли DHCP щелкните сервер правой кнопкой и выберите Properties.
2. Перейдите на вкладку DNS. Стандартные параметры интеграции DNS и DHCP, принятые по умолчанию, менять обычно не требуется (рис. 17-4).

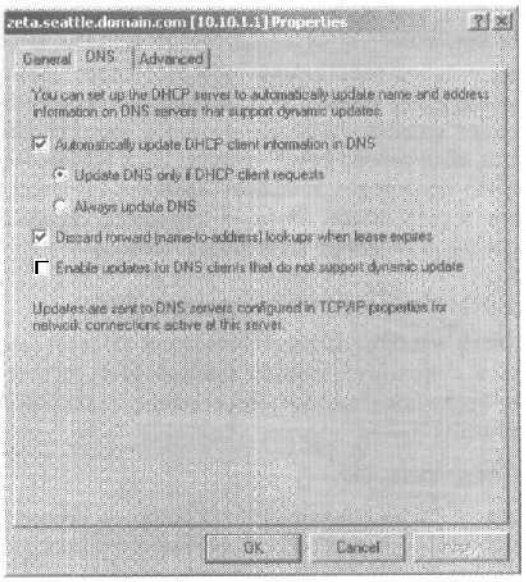


Рис. 17-4. Стандартные параметры интеграции DNS с DHCP.

Предотвращение конфликтов IP-адресов

Конфликт IP-адресов — типичная причина неполадок DHCP. Два компьютера одной сети не могут иметь одинаковых личных IP-адресов. Если компьютеру присвоен IP-адрес, уже имеющийся в сети, один или оба компьютера могут быть отключены от сети. Для удобства выявления и предотвращения потенциальных конфликтов желательно включить диагностику конфликтов IP-адресов.

1. В консоли DHCP правой кнопкой щелкните сервер и выберите Properties.
2. На вкладке Advanced задайте ненулевое значение параметру Conflict Detection Attempts (Число попыток определения конфликтов). Он определяет число проверок IP-адреса сервером (но команде ping) перед выдачей его клиенту в аренду.

Примечание Личный IP-адрес — стандартный IP-адрес сети класса A, B или C. Когда клиент запрашивает аренду, сервер проверяет пул доступных адресов и предоставляет доступный IP-адрес. По умолчанию сервер проверяет толь-

ко список адресов, уже выданных в аренду. Сеть не опрашивается для получения списка используемых адресов. В то же время в интенсивно работающей сети этот адрес может быть присвоен другому компьютеру администратором, или же к сети может подключиться компьютер с неистекшим сроком аренды, хотя сервер DHCP считает срок истекшим. В любом случае происходит конфликт адресов, вызывающий проблемы в сети. Чтобы этого не случалось, задайте число попыток распознавания конфликтов больше 0.

Сохранение и восстановление конфигурации DHCP

После настройки всех необходимых параметров DHCP вам может понадобиться сохранить конфигурацию DHCP, чтобы затем ее можно было восстановить на сервере. Для этого наберите в командной строке:

```
netsh dhcp dump >> dhcpconfig.dmp
```

Здесь dhcpconfig.dmp — имя создаваемого сценария конфигурации. Создав сценарий, вы можете восстановить конфигурацию, набрав:

```
netsh exec dhcpconfig.dmp
```

Совет Эта методика позволяет идентично настроить другой сервер DHCP: просто скопируйте сценарий в папку целевого компьютера и выполните.

Управление областями DHCP

Установив сервер DHCP, надо настроить области, которые будут использованы сервером, — пулы адресов, предоставляемые в аренду клиентам. Как уже говорилось в разделе «Понятие областей», можно создать области трех типов: суперобласти, обычные и многоадресные.

Создание и управление суперобластями

Суперобласть — это контейнер областей, напоминающий организационное подразделение к Active Directory, Суперобласть упрощает управление обычными областями сети, позволяя одним действием активизировать/отключить несколько областей. Также вы можете видеть статистику всех областей суперобласти, не проверяя каждую в отдельности.

Создание суперобластей

1. В консоли DHCP щелкните сервер правой кнопкой и выберите New Superscope (Создать суперобласть). Запустится мастер создания суперобласти.
2. Щелкните Next и введите название суперобласти.
3. Выберите области, которые нужно добавить в суперобласть, щелкнув их в списке Available Scopes (Доступные области). Можно отметить сразу несколько областей, щелкая мышью и удерживая клавишу SHIFT или CTRL.
4. Щелкните Next, а затем — Finish.

Добавление областей к суперобласти

Добавить области в суперобласть можно как при ее создании, так и после этого.

1. Щелкните выбранную область правой кнопкой и выберите Add To Superscope (Добавить в суперобласть).
2. Выберите суперобласть в окне Add Scope ... To Superscope.
3. Щелкните OK. Область добавится в суперобласть.

Удаление областей из суперобласти

1. Щелкните правой кнопкой нужную область и выберите Remove From Superscope (Удалить из супсробласти).
2. Подтвердите выбор, щелкнув Yes. Если это была последняя область суперобласти, суперобласть автоматически удаляется.

Активизация и отключение суперобласти

При активизации суперобласти одновременно активизируются/отключаются все области, входящие в нее. Для активизации/отключения суперобласти щелкните се правой кнопкой и выберите соответственно Activate (Активировать) или Deactivate (Отключить).

Удаление суперобласти

При удалении суперобласти удаляется ее контейнер и все области внутри него. Если вы не хотите удалять последние, предварительно выведите их из суперобласти.

Чтобы удалить суперобласть, щелкните ее правой кнопкой и выберите Delete (Удалить), а затем щелкните Yes для подтверждения.

Создание и управление областями

Области предоставляют пул IP-адресов клиентам DHCP. Обычные области включают в себя адреса сетей класса A, B или C, а многоадресные — области с адресами сети класса D. Хотя вы отдельно создаете обычные и многоадресные области, управлять ими можно одинаково. Главное различие между ними: к многоадресным областям неприменимо резервирование, и для них нельзя задать дополнительные параметры WINS, DNS, маршрутизацию и т. п.

Создание обычных областей

1. В консоли DHCP щелкните правой кнопкой нужный сервер. Если вы хотите автоматически добавить новую область в суперобласть, щелкните нужную суперобласть правой кнопкой.
2. В контекстном меню выберите New Scope (Создать область). Появится мастер создания новой области. Щелкните Next.
3. Введите имя и описание новой области и щелкните Next.
4. Поля Start Address (Начальный адрес) и End Address (Конечный адрес) определяют диапазон IP-адресов, которые могут входить в область. Введите значения этих полей.

Примечание Как правило, области не содержат адреса вида *x.x.x.*0 и *x.x.x.*255, которые обычно резервируются соответственно для адресов сетей и широковещательных рассылок. Поэтому вместо диапазона 192.168.10.0 — 192.168.10.255 введите 192.168.10.1 — 192.168.10.254.

5. После ввода диапазона IP-адресов битовая длина и маска подсети заполняются автоматически (рис. 17-5). Если в сети нет подсетей, используйте стандартные значения.
6. Щелкните Next. Если введенный диапазон относится к разным сетям, лучше создать суперобласть, содержащую отдельную область для каждой сети. Щелкните Yes, а затем — Next. Если вы ошиблись, щелкните Back (Назад) и измените диапазон введенных адресов.
7. В нолях Exclusion Range (Исключаемый диапазон) определите диапазоны IP-адресов, исключаемые из области. Исключить несколько диапазонов IP-адресов можно так.

- Чтобы определить исключенный диапазон, введите адреса в полях Start Address (Начальный адрес) и End Address (Конечный адрес) и щелкните Add (Добавить). Для исключения единичного адреса введите его значение в обоих полях.
- Исключенные адреса **отображаются *в* списке** Excluded **Addresses (Исключаемые** адреса).
- Чтобы удалитьисключенный диапазон, выберите его в списке Excluded Addresses и щелкните Remove (Удалить).

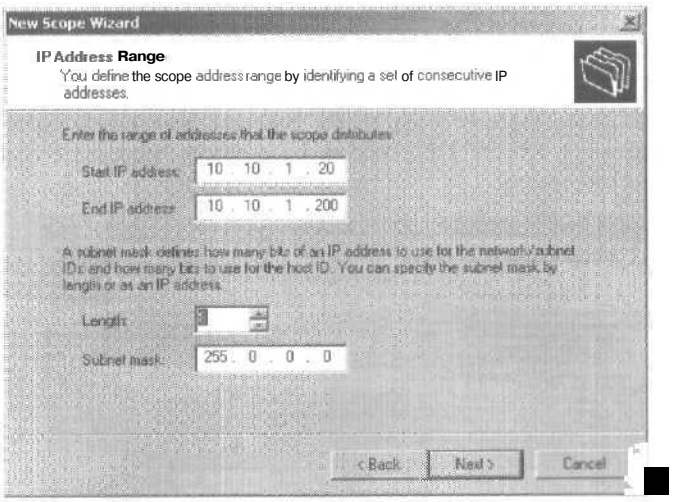


Рис. 17-5. В окне мастера создания области введите диапазон IP-адресов новой области.

8. Выберите продолжительность аренды для области, заполнив поля Day(s) (Дни), Hour(s) (Часы) и Minutes (Минуты); по умолчанию — 8 дней.

Совет Слишком большой срок аренды может привести к снижению эффективности DHCP и исчерпанию доступных IP-адресов, особенно если в сети работает много мобильных или иных пользователей, не являющихся постоянными членами сети. Оптимальный срок аренды для большинства сетей — 1-3 суток.

9. Теперь можно настроить параметры DHCP для DNS, WINS, шлюзов и т. п. Если вы хотите это сделать, щелк-

ните Yes. В противном случае щелкните No и пропустите пп. 10–16.

10. Щелкните Next. Первое, что нужно настроить, — стандартный шлюз. В поле IP-адреса введите IP-адрес первичного шлюза по умолчанию. Щелкните Add (Добавить). Повторите эту процедуру для остальных стандартных шлюзов.
11. Клиенты сначала будут пытаться использовать первый шлюз в списке. Если он недоступен, они обратятся к следующему шлюзу и т. д. Вы можете изменить порядок расположения шлюзов в списке клавишами-стрелками «вверх» и «вниз».
12. Щелкните Next. Настройте стандартные параметры DNS клиента DHCP (рис. 17-6). Введите имя родительского домена, чтобы DNS могла разрешить неполные имена компьютеров.

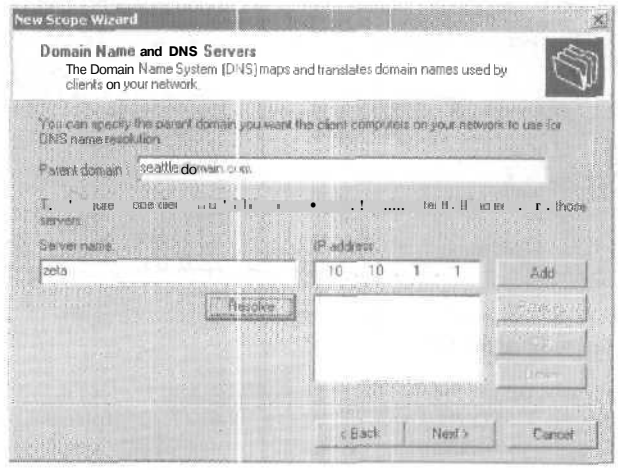


Рис. 17-6. Настройка стандартных параметров DNS для клиентов DHCP.

13. В поле IP Address введите IP-адрес первичного DNS-сервера. Щелкните Add. Повторите процедуру для дополнительных серверов DNS. Расположение IP-адресов в списке определяет очередность обращения к ним. Можете также изменить порядок адресов «кнопками-стрелками».

Совет Если вам известно имя сервера, но не его IP-адрес, введите это имя в поле Server Name и щелкните Resolve (Разрешить). При успешном разрешении значение IP-адреса появится в поле IP Address. Добавьте сервер, щелкнув Add.

14. Аналогично настройте стандартные параметры WINS для клиентов DHCP.
15. Чтобы активизировать область, щелкните Yes, I Will Activate This Scope Now (Активизировать эту область сейчас) и Next, иначе просто щелкните Next.
16. Завершив создание областей. щелкните Finish (Готово).

Создание многоадресных областей

1. В консоли DHCP щелкните правой кнопкой значок сервера, на котором хотите создать многоадресную область. Если хотите добавить область к существующей суперобласти, щелкните последнюю правой кнопкой.
2. В контекстном меню выберите New Multicast Scope (Создать многоадресную область) — запустится мастер создания многоадресной области. Щелкните Next.
3. Введите имя и описание новой области и щелкните Next.
4. Поля Start Address (Начальный адрес) и End Address (Конечный адрес) определяют диапазон IP-адресов, которые могут входить в область. Заполните эти поля.
5. Рассылаемые компьютерами пакеты с широковещательными адресами характеризуются таким параметром, как время жизни (time-to-live). Время жизни пакета равно максимальному числу маршрутизаторов, через которые он может пройти. Стандартное значение — 32, чего достаточно для большинства сетей. В большой сети может понадобиться его увеличить в соответствии с имеющимся количеством маршрутизаторов.
6. Щелкните Next. Если вы ошиблись, щелкните Back и измените значение диапазона.
7. Заполнив поля Exclusion Range, определите диапазоны IP-адресов, которые не будут включены в область. Можно исключить несколько диапазонов адресов.
   - Чтобы определить исключенный диапазон, введите адреса в полях Start Address (Начальный адрес) и End

Address (Конечный адрес) и щелкните Add (Добавить). Для исключения единичного адреса введите его значение в обоих полях.

- Исключенные адреса отображаются в списке Excluded Addresses (Исключаемые адреса).
- Чтобы удалить исключенный диапазон, выберите его в списке Excluded Addresses и щелкните Remove (Удалить).

8. Задайте **продолжительность аренды области в полях** Day(s), **Hour(s)** и Minutes; **по умолчанию — 30 дней.**

Примечание Если вы недостаточно компетентны в вопросах широковещательной рассылки, не меняйте стандартное значение. Многоадресная аренда используется не так, как обычная. Широковещательный IP-адрес могут применять несколько компьютеров, и все они могут иметь права аренды этого IP-адреса. Рекомендуемая длительность многоадресной аренды в большинстве сетей — 30-60 дней.

9. Если хотите сейчас активизировать область, щелкните Yes, иначе щелкните Next.
10. Закончив создание областей, щелкните Finish.

Настройка параметров областей

Параметры области позволяют тонко управлять се работой и задавать стандартные параметры клиентов TCP/IP, использующих область. Так, вы можете разрешить клиентам автоматически находить в сети серверы DNS. Кроме того, вы можете определить параметры стандартных шлюзов, WINS и т. п. Параметры области применимы только к обычным областям, но не к многоадресным.

Вы можете определить параметры областей:

- глобально для всех областей, настроив стандартные параметры сервера;
- для области, настроив параметры области;
- для клиента. настроив параметры резервирования;
- для клиента, сконфигурировав классы, определяемые поставщиком или клиентом.

Параметры области расположены иерархически, что определяет, какой именно г араметр будет действовать. Порядок

расположения соответствует очередности в списке выше. Фактически это значит, что:

- параметры области преобладают нал глобальными параметрами;
- параметры клиента преобладают над параметрами области и глобальными;
- параметры класса преобладают над всеми остальными.

Просмотр и назначение параметров сервера Параметры сервера относятся ко всем областям, созданным на отдельном сервере DHCP. Вы можете посмотреть их и внести изменения.

1. В консоли DHCP двойным щелчком откройте нужный сервер.
2. Для просмотра параметров щелкните Server Options (Параметры сервера). В правой панели будут показаны текущие параметры.
3. Для перенастройки параметров щелкните *правой* кнопкой Server Options и выберите Configure Options (Настроить параметры). В открывшемся диалоговом окне Server Options отметьте флажком нужный параметр и заполните необходимые поля в панели ввода данных. Повторите эти действия для остальных параметров.

Просмотр и настройка параметров областей Эти параметры специфичны для каждой области и имеют приоритет над стандартными параметрами сервера. Их можно просмотреть и изменить.

1. Откройте нужную область в консоли DHCP.
2. Для просмотра параметров щелкните Scope Options (Параметры области). В правой панели будут показаны текущие параметры.
3. Для изменения параметров щелкните правой кнопкой Scope Options и выберите Configure Options. Откроется окно настройки параметров области. Отметьте флажком нужный параметр и заполните необходимые поля в панели ввода данных. Повторите эти действия для каждого настраиваемого параметра.

Просмотр и настройка параметров резервирования Эти параметры относятся к клиенту, за которым резервируется IP-адрес. Они специфичны для каждого клиента и имеют при-

оритет над параметрами сервера и области. Параметры резервирования можно установить и просмотреть.

1. Откройте нужную область в консоли DHCP.
2. Дважды щелкните папку Reservations (Резервирование) нужной области.
3. Щелчок объекта резервирования выводит его текущие параметры конфигурации в правой панели.
4. Чтобы их изменить, щелкните объект правой кнопкой и выберите Configure Options (Параметры). В открывшемся диалоговом окне Reservation Options (Параметры резервирования) отметьте флажком настраиваемый параметр и введите нужные значение полей в панели ввода данных. Повторите эти действия для других параметров.

Изменение **областей**

1. Откройте консоль DHCP и дважды щелкните сервер, который хотите настроить. Появятся настраиваемые области данного сервера.
2. Щелкните правой кнопкой нужную область и выберите Properties (Свойства).
3. Для обычной области можно не ограничивать срок аренды, но при постоянной аренде снижается эффективность пула IP-адресов, выделяемых DHCP. Постоянная аренда не будет прекращена, пока вы явно ее не отмените или не отключите область. В результате вы можете остаться без свободных адресов, особенно по мере роста сети. Альтернатива постоянной аренде — резервирование адресов, но только для отдельных клиентов, которым нужны постоянные IP-адреса.
4. Для многоадресных областей можно задать время жизни, т. е. сколь долго область действительна. По умолчанию многоадресные области существуют, пока активны. Для изменения этого значения на вкладке Advanced (Дополнительно) щелкните Multicast Scope Expires On (Срок действия многоадресной области истекает) и введите дату окончания действия.
5. Закончив изменения, щелкните OK. Изменения сохранятся в консоли DHCP.

Активизация и отключение областей

В консоли DHCP неактивные области помечены значком с красной стрелкой-вниз, а активные — значком обычной папки.

Активизировать область можно в консоли **DHCP,** щелкнув ее **правой** кнопкой и выбрав Active.

Отключить область можно в консоли DHCP, щелкнув ее правой кнопкой и **выбрав** Deactive.

Совет Деактивация отключает область, но не прекращает текущую аренду клиентов. О прекращении аренды см. **раздел** «Высвобождение адресов и аренды».

Применение протокола BOOTP

BOOTP — протокол динамической адресации, предшествующий DHCP. Обычные области его не поддерживают. Протокол начальной загрузки включается так.

1. Щелкните правой кнопкой модифицируемую область и выберите Properties.
2. На вкладке Advanced (Дополнительно) щелкните Both (Оба) для поддержки клиентов DHCP и BOOTP.
3. Можно также задать продолжительность аренды клиента BOOTP. Щелкните OK.

Удаление области

При удалении область навсегда удаляется с сервера DHCP.

1. В консоли DHCP щелкните правой кнопкой удаляемую область и выберите Delete.
2. Подтвердите удаление области, щелкнув Yes.

Настройка нескольких областей сети

В одной сети можно настроить несколько областей. Их могут обслуживать один или несколько серверов DHCP. Во вре.мя работы с несколькими областями чрезвычайно важно помнить, что диапазоны адресов, используемые разными областями, не могут перекрываться. Каждая область должна владеть уникальным диапазоном адресов, иначе один и тот же IP-адрес может быть выдан различным клиентам DHCP, что может помешать работе сети.

Рассмотрим пример. На сервере А вы создаете область с диапазоном 192.168.10.1-192.168.10.99, на сервере В - с ди-

апазоном 192.168.10.100–192.168.10.199, на сервере С — с диапазоном 192.168.10 100-192.168.10.199. Каждый из этих серверов может отвечать на сообщения о запросе аренды DHCP и присваивать IP-адреса клиентам. При отказе одного из них остальные будут обслуживать сеть.

Управление пулом адресов, арендой и резервированием

В областях есть отдельные каталоги для пулов адресов, аренды и резервирования, позволяющие посмотреть текущую статистику и управлять элементами.

Просмотр статистики области

Статистика области показывает общую информацию об адресном пуле текущей области или. суперобласти. Чтобы посмотреть статистику, щелкните правой кнопкой интересующую область или суперобласть и выберите Display Statistics (Отобразить статистику). Появится диалоговое окно (рис. 17-7).

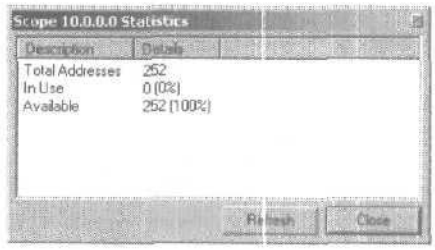


Рис. 17-7. В окне статистики отражена общая информация о пуле адресов текущей области или суперобласти.

- **Total Addresses (Всего адресов) — количество IP-адресов, присвоенных области.**
- In Use (Используется) — количество адресов, используемых в настоящее время. Показана абсолютная величина и процентное отношение к общему числу доступных адресов. Если это отношение — 85% и более, увеличьте количество доступных адресов или освободите занятые.
- Available (Доступно) — количество доступных для использованию адресов. Показана абсолютная величина и процент к общему числу доступных адресов.

Настройка нового диапазона исключений

Можно исключить IP-адреса из области, определив диапазон исключений. Область может содержать несколько таких диапазонов. Чтобы настроить новый диапазон исключений, сделайте так.

1. В консоли DHCP откройте нужную область, щелкните правой кнопкой папку Address Pool (Пул адресов) и выберите New Exclusion Range (Создать исключенный диапазон).
2. Последовательно введите начальный и конечный адрес диапазона и щелкните Add (Добавить). Выбранный диапазон должен находится в пределах диапазона адресов данной области и не должен использоваться в данный момент. Повторите эти действия для добавления других диапазонов исключений.
3. Щелкните Close.

Удаление диапазона исключений

Исключение можно удалить, щелкнув его правой кнопкой и выбрав Delete (Удалить).

Согласование аренды и резервирования

Для согласования аренды и резервирования щелкните правой кнопкой нужную область и выберите Reconcile (Согласовать). При согласовании аренда клиентов и резервирование сравнивается с БД DHCP па сервере. Это полезно, если вы хотите убедиться, что отображаемый список аренды действительно используется.

Резервирование адресов DHCP

Присвоить клиентам постоянные адреса в DHCP можно несколькими способами. Например, включить параметр Unlimited в диалоговом окне области, чтобы дать постоянные адреса всем клиентам этой области. Или: зарезервировать адреса DHCP за клиентами. При резервировании адреса DHCP клиент всегда получает один и тот же IP-адрес от DHCP-сервера, при этом вы не жертвуете централизацией управления, которое делает столь привлекательной технологию DHCP.

Вот как зарезервировать DHCP-адреса за клиентом.

1. В консоли DHCP откройте нужную область, щелкните правой кнопкой папку Reservations (Резервирование) и выберите New Reservation (Создать резервирование). Откроется одноименное диалоговое окно (рис. 17-8).

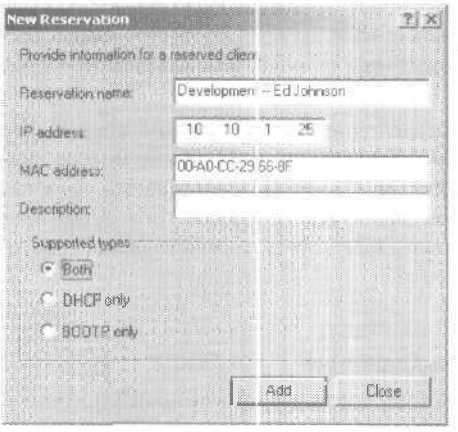


Рис. 17-8. Резервирование IP-адреса для клиента.

2. В поле Reservation Name (Имя резервирования) наберите короткое описательное название резервирования. Это поле служит только для идентификации.
3. В поле IP Address введите IP-адрес, который хотите зарезервировать за клиентом. Он должен находиться в действительном диапазоне адресов выбранной области.
4. Поле MAC Address определяет адрес протокола Media Access Control (MAC) для сетевого адаптера компьютера клиента. Узнать MAC-адрес можно, набрав в командной строке компьютера клиента команду **IPCONFIG** /ALL: MAC-адрес клиента указан и разделе Physical Address (Физический адрес). Это значение следует вводить *точно,* иначе резервирование работать не будет.
5. По желанию введите комментарий в поле Description (Описание).
6. По умолчанию поддерживаются клиенты DHCP и BOOTP. Этот параметр относится к тонкой настройке и нужен, только когда нужно исключить конкретный тип клиентов.
7. Щелкните Add для резервирования.

Высвобождение адресов и аренды

Вы должны знать ряд ограничений работы с зарезервированными адресами.

- Зарезервированные адреса не могут переназначаться автоматически. Поэтому, если адрес уже используется, освободите его, чтобы клиент мог его задействовать. Вы можете заставить клиента освободить адрес, прекратив аренду или набрав на компьютере клиента в командной строке **IPCONFIG /RELEASE.**
- Клиенты не могут автоматически переходить на зарезервированный адрес. Поэтому, если клиент владеет другим IP-адресом, нужно заставить освободить его и запросить новый. Это можно также сделать, прекратив аренду или набрав на компьютере клиента в командной строке **IPCONFIG** /RENEW.

Изменение свойств резервирования

1. В консоли DHCP откройте нужную область и щелкните папку Reservations.
2. Щелкните резервирование правой кнопкой и выберите Properties. Теперь можно изменить свойства резервирования. Затененные поля нельзя изменить, остальные — можно. Поля соответствуют описанным в прошлом разделе.

Удаление аренды и резервирования

1. В консоли DHCP откройте нужную область и щелкните папку Address Leases (Аренда адресов) или Reservations.
2. Щелкнув правой кнопкой аренду или удаляемое резервирование, выберите Delete.
3. Подтвердите удаление, щелкнув Yes.
4. Аренда или резервирование будут удалены из DHCP. Впрочем, клиент при этом может и не освободить IP-адрес. Чтобы заставить его сделать это. на компьютере клиента наберите в командной строке **IPCONFIG /RELEASE.**

Резервное копирование и восстановление БД DHCP

Серверы DHCP хранят данные об аренде и резервировании DHCP в файлах БД. По умолчанию они находятся в папке

%SystemRoot%\System32\dhcp. Ключевые файлы этого каталога:

- **DHCP.MDB** - основной файл БД сервера DHCP;
- **DHCP.TMP** — временный рабочий файл сервера DHCP;
- **J50.LOG** — файл журнала операций, служит для восстановления незаконченных операций при отказе сервера;
- **J50.CHK** — файл контрольной точки, применяемый для усечения файла журнала сервера DHCP

Каталог резервного копирования

Каталог *%SystemRoot%*\System32\dhcp хранит резервные данные о настройке DHCP и БД DHCP. По умолчанию БД сохраняется каждые 60 минут. Параметры рееетра, отвечающие за размещение резервной копии и периодичность сохранения данных DHCP, и другие параметры DHCP хранятся в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

Восстановление БД DHCP из резервной копии

1. Остановите службу сервера DHCP. Раскройте узел Services And Applications Б консоли Computer Management или дважды щелкните ярлык DHCP в меню Administrative Tools. Щелкнув правой кнопкой сервер DHCP, выберите All Tasks (Все задачи), а затем — Stop (Остановить).
2. Восстановите рабочую копию папки *%SystemRoot%*\System32\dhcp\backup с ленточного накопителя или другого архивного устройства.
3. В редакторе реестра откройте раздел HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters. Присвойте параметру RestoreFlag значение 1.
4. Запустите службу сервера DHCP. Помните, что может потребоваться повторная авторизация DHCP. Если на значке DHCP — красная «стрелка-вниз», щелкните значок сервера DHCP правой кнопкой и выберите Authorize (Авторизовать).

Глава 18

Поддержка WINS

Служба имен Интернета для Windows (Windows Internet Naming Service, WINS) разрешает (преобразует) имена компьютеров в IP-адреса. При использовании WINS имя компьютера OMEGA, к примеру, может быть разрешено в IP-адрес, позволяющий компьютерам в сети Microsoft находить друг друга и передавать информацию. WINS необходима для поддержки систем, более ранних, чем Windows 2000, и старых приложений, использующих NetBIOS поверх TCP/IP, таких как команда командной строки NET. Если у вас в сети нет ранних версий Windows и требующих совместимости с ними приложений, WINS вам не нужна.

NetBIOS — это интерфейс прикладного программирования (application programming interface, API), обеспечивающий разрешение имен WINS и передачу информации между компьютерами. API-интерфейс NetBIOS содержит набор команд, которые приложения могут задействовать для доступа к службам сеансового уровня. Обычно используются такие расширения NetBIOS: улучшенный интерфейс пользователя NetBIOS (NetBIOS Enhanced User Interface, NetBEUI) и NetBIOS поверх TCP/IP (NetBIOS over TCP/IP, NBT). Мы рассмотрим WINS и NBT.

В Windows 2000 WINS не устанавливается автоматически. Поэтому вы должны сделать следующее.

1. Щелкните Start (Пуск), выберите Settings (Настройка), а затем — Control Panel (Панель управления).
2. Дважды щелкните значок Add/Remove Programs (Установка и удаление программ).
3. Щелкните Add/Remove Windows Components (Установка и удаление компонентов Windows), а затем — Next (Далее).

4. Прокрутите список Components (Компоненты) до пункта Networking Services (Сетевые службы) и щелкните его.
5. **Щелкните** Details **(Состав).**
6. В списке Subcomponents щелкните Windows Internet Naming Service (WINS), а затем — OK.
7. Если появится запрос, введите полный путь к установочным файлам Windows 2000 и щелкните Continue (Продолжить).

Примечание Сервер WINS должен иметь статический **IP-адрес.**

Понятие WINS и NetBIOS поверх TCP/IP

WINS работает в системе клиент — сервер, где клиенты WINS посылают к WINS-серверам запросы на разрешение имени, а WINS-серверы обрабатывают запрос и отвечают. Для передачи запросов WINS и другой информации компьютеры используют NetBIOS. NetBIOS обеспечивает API, позволяющий компьютерам в сети связываться друг с другом. Когда вы устанавливаете протокол TCP/IP у клиента или сервер сети Microsoft, также устанавливается поддержка NetBIOS поверх TCP/IP. NetBIOS поверх TCP/IP — это служба сеансового уровня, позволяющая приложениям NetBIOS работать через стек протокола TCP/IP. Приложения NetBIOS полагаются на WINS или локальный файл LMHOSTS для разрешения имен компьютеров в IP-адреса.

В более ранних по сравнению с Windows 2000 сетях WINS являлся основной службой разрешения имен. В сетях Windows 2000 эта роль отдана системе доменных имен (Domain Name System, DNS), а WINS обеспечивает устаревшим системам просмотра список ресурсов сети и занимается поиском ресурсов NetBIOS для систем на базе Windows 2000.

Настройка клиентов и серверов WINS

Для разрешения имен WINS в сети вам нужно настроить клиенты и серверы WINS. Настраивая клиенты WINS, вы сообщаете им IP-адреса WINS-серверов в сети. По этим IP-адресам клиенты могут связываться с WINS-серверами во всей сети, даже если серверы находятся в других подсетях. Клиенты также могут связываться путем широковещатель-

ных запросов IP-адресов компьютеров внутри сегмента локальной сети. Любые не-WINS клиенты, поддерживающие этот тип широковещательных сообщений, также могут использовать этот метод для разрешения имен компьютеров в IP-адреса.

Связываясь с WINS-серверами, клиенты устанавливают сеансы, в которых можно выделить три ключевых этапа.

- Регистрация имени. В процессе регистрации имени клиент сообщает серверу имя своего компьютера и его IP-адрес и просит включить эту информацию в БД WINS. Если имя и IP-адрес не используются другим компьютером в сети, WINS-сервер принимает запрос и регистрирует клиента в БД WINS.
- Обновление имени. Имя регистрируется не навсегда. Клиент использует его в течение определенного периода, называемого временем аренды. Клиенту также дается интервал обновления, в течение которого аренда должна быть обновлена. За это время клиент должен перерегистрироваться на WINS-сервере.
- Освобождение имени. Если клиент не может обновить аренду, зарегистрированное имя освобождается, что позволяет другим системам в сети использовать то же имя компьютера или IP-адрес. Имя также освобождается, когда вы завершаете работу WINS-клиента.

Примечание О настройке WINS-клиента см. главу 15, о настройке WINS-сервера — раздел «Настройка WINS-серверов».

Методы разрешения имени

Соединившись с WINS-сервером, клиент может обращаться с запросами к службам разрешения имен. Метод разрешения имен компьютеров в IP-адреса зависит от настройки сети. Существует четыре метода разрешения имен.

- **B-node** (broadcast node, широковещательный запрос узла) использует широковещательные сообщения для разрешения компьютерных имен в IP-адреса. Компьютеры, которым нужно разрешить имя, рассылают широковещательное сообщение каждому узлу в локальной сети с запросом IP-адреса по имени компьютера.

- **P-node** (point-to-point node, запрос узла «точка — точка») использует WINS-серверы для разрешения имен компьютеров в IP-адреса. Как сказано выше, клиентские сеансы подразделяются на три этапа: регистрация имени, обновление имени и освобождение имени. Когда клиенту нужно разрешить имя компьютера в IP-адрес, клиент отправляет запрос серверу и тот отвечает.
- **M-node** (modified node, модифицированный запрос узла) комбинирует запросы b- и p-node. При использовании этого типа запроса WINS-клиент пытается применить b-node, а в случае неудачи — p-nodc. Поскольку первым используется b-node, данный метод также серьезно нагружает сеть широковещательным трафиком, как и b-node.
- **H-node** (hybrid node, гибридный запрос узла) также совмещает запросы b-node и p-node. При этом WINS-клиент сначала пытается использовать запрос типа p-node для разрешения имени через соединение «точка — точка». В случае неудачи клиент пытается использовать широковещательное сообщение b-node. Поскольку сначала применяется метод «точка — точка», h-node работает быстрее в большинстве сетей. Метод h-node используется по умолчанию для разрешения имен WINS.

Если в сети доступны WINS-серверы, клиенты Windows используют метод p-node для разрешения имени. Если в сети нет доступных WINS-серверов, клиенты Windows 2000 используют метод b-node для разрешения имени. Компьютеры Windows также могут использовать DNS и локальные файлы LMHOSTS и HOSTS для разрешения сетевых имен. О работе с DNS см. главу 19.

Совет Используя для динамического назначения IP-адресов протокол динамической настройки узлов (Dynamic Host Configuration Protocol, DHCP), вы должны задать метод разрешения имен для клиентов DHCP. Для этого задайте параметры области действия DHCP для типа узла — 046 WINS/NBT (см. главу 17). Лучше всего использовать метод h-node, который дает наивысшую производительность и меньше нагружает сеть.

КонсольWINS

Вы можете просмотреть и изменить параметры сервера ил консоли WINS.

Знакомство с консолью WINS

Для управления WINS-сервером в сети служит консоль WINS (рис.18-1) из папки Administrative Tools (Администрирование). Ее главное окно разделено на две панели. В левой перечислены WINS-серверы в домене по их IP-адресам, в том числе и локальные компьютеры, если они — WINS-серверы.

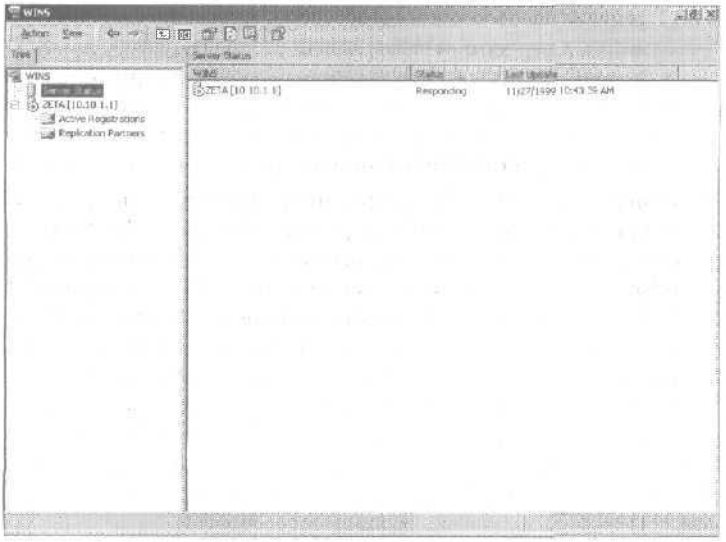


Рис. 18-1. Для настройки WINS-сервера служит консоль WINS.

Дважды щелкнув запись в левой панели, вы раскроете список, показывающий папки Active Registrations (Активные регистрации) и Replication Partners (Партнеры репликации). Папка Active Registrations отображает информацию о статусе зарегистрированных имен компьютеров. Папка Replication Partners содержит сводную информацию о WINS-серверах, с которыми данный сервер обменивается регистрационной информацией.

Добавление WINS-сервера на консоль WINS

Если в списке на консоли WINS нет того WINS-сервера, который вы хотите настроить, вы можете его добавить.

1. Щелкните правой кнопкой WINS в дереве консоли и выберите Add Server (Добавление сервера).

2. Введите IP-адрес или имя WINS-сервера, которым собираетесь управлять.
3. Щелкните OK. Запись для этого WINS-сервера добавится в дерево консоли.

Примечание Вы также можете управлять локальным и удаленными WINS-серверами из консоли Computer Management (Управление компьютером). Запустите ее и подключитесь к серверу, которым хотите управлять. Затем раскройте узел Services And Applications (Службы и приложения) и выберите WINS.

Запуск и остановка WINS-сервера

Управление WINS-серверами производится через службу имен Интернета Windows. Как и любую другую, ее можно запускать, останавливать, временно приостанавливать и перезапускать из узла Services консоли Computer Management или из командной строки. Для управления WINS-серверами из Computer Management щелкните правой кнопкой WINS, выберите All Tasks (Все задачи), а затем — Start (Запустить), Stop (Остановить), Pause (Приостановить), Resume (Возобновить) или Restart (Перезапустить). Вы также можете управлять WINS из консоли WINS: щелкните правой кнопкой сервер, которым хотите управлять, выберите All Tasks, а затем — Start, Stop, Pause, Resume или Restart.

Просмотр статистики сервера

Статистика сервера дает сводную информацию о WINS, которая может пригодиться при управлении и устранении неисправностей WINS. Для просмотра статистики сервера в консоли WINS щелкните правой кнопкой сервер и выберите Display Server Statistics (Отобразить статистику сервера). Статистика отображается в сводном формате (рис. 18-2).

Статистика содержит следующую информацию.

- **Server Start Time** (Время запуска сервера) — время, когда на сервере была запущена WINS.
- **Database Initialized** (База данных проинициализирована) — время, когда была инициализирована БД WINS на сервере.
- Statistics **Last Cleared** (Статистика очищена в последний раз) — время, когда в последний раз была очищена статистика сервера.

- **Last Periodic Replication** (Последняя **репликация по** расписанию) — время, когда БД WINS была в последний раз реплицирована но истечении временного интервала репликации, заданного в окне Pull Partner Properties.
- Last Manual Replication (Последняя репликация вручную) — время, когда БД WINS была в последний раз реплицирована администратором.
- **Last Net Update Replication (Последняя репликация** изменения состояния сети) — время, когда БД WINS была в последний раз реплицирована на основании полученного из сети уведомления, запросившего передачу.
- Last Address Change Replication (Последнее репликация изменения адреса) — время, когда БД WINS была в последний раз реплицирована па основании сообщения об изменении адреса.
- Total Queries (Всего запросов) — общее число запросов, принятых сервером с момента последнего запуска. Поле Records Found (Найдено записей) показывает число успешно разрешенных запросов, поле Records Not Found (Не найдено записей) — число неудовлетворенных запросов.
- Total Releases (Всего освобождено) — общее число принятых сообщений о том, что приложение NetBIOS освободило зарезервированное имя и отключилось. Поле Records Found показывает число успешно выполненных освобождений, поле Records Not Found — число неудачных освобождений.

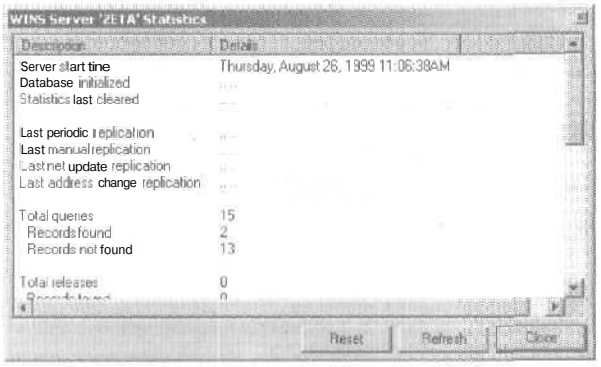


Рис. 18-2. Статистика WINS дает информацию, полезную для контроля и устранения неисправностей этой службы.

- **Unique** Registrations (Уникальные регистрации) — общее количество полученных и удовлетворенных сообщений от клиентов WINS о регистрации имени. Поле Conflicts (Конфликты) показывает число конфликтов имен, зафиксированных для каждого уникального имени компьютера, поле Renewals (Обновления) — число обновлений, зафиксированных для каждого уникального имени компьютера.
- **Group Registrations** (Регистрации группы) — общее количество полученных и удовлетворенных сообщений от групп о регистрации имени. Поле Conflicts показывает число конфликтов имен, зафиксированных для имен групп, поле Renewals — число обновлений, зафиксированных для имен групп.
- Total **Registrations** (Всего регистрации) — общее количество сообщений о регистрации имени принятых от клиентов WINS.
- **Last Periodic Scavenging** (Последняя автоматическая очистка) — время последней очистки по причине истечения интервала обновления, заданного в окне WINS Server Configuration (Настройка WINS-сервера).
- **Last Manual Scavenging** (Последняя очистка вручную) — время последней очистки по запросу администратора.
- **Last Extinction Scavenging** (Время последнего окончания очистки) — время последней очистки по причине истечения интервала удаления, заданного в окне WINS Server Configuration.
- **Last Verification Scavenging** (Время последней проверки очистки) — время последней очистки по причине истечения интервала проверки, заданного в окне WINS Server Configuration.

Настройка WINS серверов

Когда вы устанавливаете WINS-сервер, он настраивается со стандартными параметрами. Вы можете их изменить.

1. В консоли WINS щелкните правой кнопкой сервер, с которым хотите работать и выберите Properties (Свойства). Появится диалоговое окно (рис. 18-3).
2. Измените значения параметров на вкладках General (Общие), Interval (Интервал), Database Verification (Проверка

базы данных) и Advanced (Дополнительно), как описано в следующих разделах.

3. Щелкните OK, когда закончите вносить изменения.

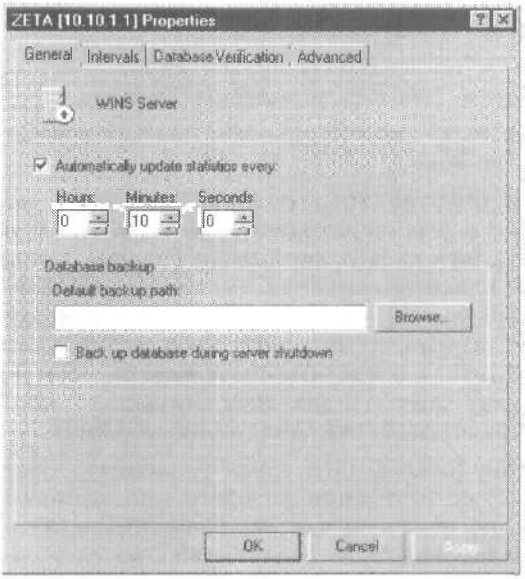


Рис. 18-3. Окно свойств для настройки WINS-сервера.

Обновление статистики WINS

Консоль WINS выводит статистику регистрации и репликации адресов. По умолчанию она обновляется каждые 10 минут. Вы можете изменить интервал обновления или вообще остановить автоматическое обновление.

1. В консоли WINS щелкните правой кнопкой сервер, с которым хотите работать, и выберите Properties.
2. Перейдите на вкладку General.
3. Чтобы задать интервал обновления, выберите Automatically Update Statistics Every (Автоматически обновлять статистику каждые) и введите значение интервала в часах, минутах и секундах.
4. Для остановки автоматического обновления снимите флажок Automatically Update Statistics Every и щелкните OK.

Управление регистрацией, обновлением и освобождением имен

Имена компьютеров регистрируются в БД WINS на период аренды. Задавая интерналы обновления, удаления и проверки, вы можете управлять параметрами аренды.

1. В консоли WINS щелкните правой кнопкой сервер, с которым хотите работать, и выберите Properties.
2. Откройте вкладку Interval (рис.18-4) на которой расположены такие поля.
   - **Renewal Interval** (Интервал обновления) — задаст интервал, в течение которого клиент WINS должен обновить имя своего компьютер (период аренды). Обычно клиенты пытаются выполнить обновление, когда проходит 50% времени периода аренды. Минимальное значение — 40 минут. Значение по умолчанию — 6 дней, т. с. клиенты будут пытаться возобновлять аренду каждые 3 дня. Имя компьютера, которое не было обновлено, считается освобожденным.
   - **Extinction Interval** (Интервал удаления) — задает интервал, по истечении которого имя компьютера может быть отмечено, как удаленное. После того как имя компьютера было освобождено, на следующем этапе оно будет помечено, как удаленное. Это значение должно быть больше или равно меньшему из двух значений: интервал обновления или 4 дня.
   - Extinction **Timeout** (Время простоя при удалении) — задает интервал, в течение которого имя компьютера может быть физически удалено из БД WINS. После того как имя компьютера было отмечено как удаленное, следующим шагом будет исключение его из БД. Значение по умолчанию — 4 дня.
   - **Verification** Interval (Интервал проверки) — задает интервал, по истечении которого WINS-сервер должен проверить старые имена, которыми он не владеет. Если эти имена неактивны, их можно удалить. Минимальное значение — 24 дня. Обычно имена компьютеров, зарегистрированные на другом WINS-сервере, имеют другого владельца и таким образом попадают в эту категорию.

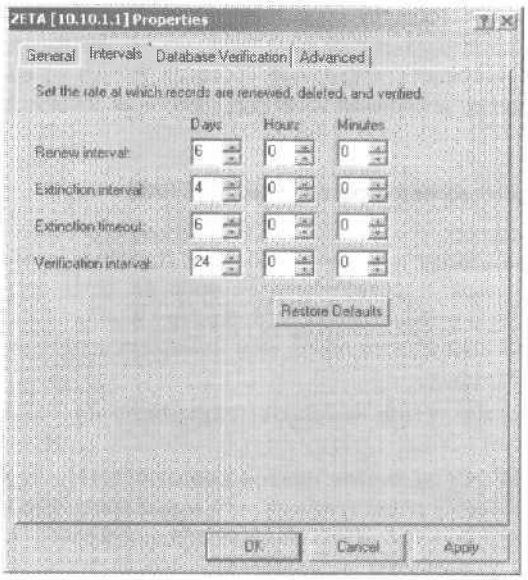


Рис. 18-4. Настройка интервалов согласно параметрам вашей сети.

Совет Эти интервалы можно представить как время жизни имен, перечисленных в БД WINS. Интервал обновления действует, когда аренда обновляется. Интервал удаления действует, когда необновленные имена помечаются как удаленные. Задержка удаления действует, когда устаревшие имена исключаются из БД. Если вы задали интервал обновления 24 часа, интервал удаления — 48 часов, а задержку удаления — 24 часа, потребуется в общей сложности 96 часов, чтобы запись была стерта из БД WINS.

Запись событий WINS в журналах Windows

События WINS записываются *а* системный журнал автоматически. Вы не можете выключить эту возможность, по вправе временно включить подробную запись в журнал, что может помочь устранить неполадки WINS.

1. В консоли WINS щелкните правой кнопкой сервер, с которым хотите работать, и выберите Properties.
2. Откройте вкладку Advanced (Дополнительно) и выберите Log Detailed Events To The Windows Event Logs.

Примечание Ведение подробного протокола в активной сети может серьезно повысить нагрузку на WINS-сервер. Поэтому включайте подробный протокол только во время тестирования, устранения неисправностей или оптимизации работы.

Настройка идентификатора версии БД WINS

Идентификатор версии для БД WINS обновляется автоматически при внесении изменений. Если БД WINS повреждается и вы хотите восстановить ее во всей сети, нужно получить доступ к основному WINS-серверу и задать значение идентификатора версии выше, чем номера версий на всех удаленных партнерах.

Вы можете просмотреть и изменить текущий номер идентификатора версии.

1. В консоли WINS щелкните правой кнопкой Active Registrations (Активные регистрации), затем выберите Find By Owner (Найти по владельцу). Появится одноименное окно.
2. На вкладке Owners (Владельцы) в колонке Highest ID (Наибольший номер) отображается наивысший номер идентификатора версии, используемый на каждом сервере. Значение показано в шестнадцатеричном формате; максимальное значение — 2^31.
3. Запомните значение наивысшего идентификатора версии и щелкните Cancel (Отмена).
4. Щелкните правой кнопкой запись основного WINS-сервера в дереве консоли, а затем выберите Properties.
5. На вкладке Advanced (Дополнительно) введите новое значение в поле Starting Version ID (Начальный номер версии). Это значение должно быть введено в шестнадцатеричном формате, например E8B, и оно должно быть больше, чем значение, которое вы запомнили ранее. Щелкните OK.

Настройка пакетной обработки регистрации имен

Зачастую на WINS-сервере одновременно пытаются зарегистрироваться несколько клиентов WINS. Иногда это может перегрузить WINS-сервер, особенно если сразу сотни компьютеров пытаются зарегистрироваться одновременно. При этом WINS-сервер может переключиться в режим пакетной

обработки, в котором он дает положительный ответ на запросы клиентов еще до того, как обработает их и внесет изменения в БД WINS.

Вы можете изменить порог включения режима пакетной обработки для приведения в соответствие размера вашей сети и мощности сервера. По умолчанию этот порог достигается, когда более чем 500 регистрации и запросов имен находятся в очереди на обработку. Новое значение порога задается так.

1. В консоли WINS щелкните правой кнопкой сервер, с которым хотите работать, и выберите Properties.
2. На вкладке Advanced убедитесь, что выбрано Enable Burst Handling (Включить обработку пакетов), а затем настройте новый порог в полях:
   - Low (Низкий) — задает порог в 300 регистрации и запросов имен;
   - **Medium** (Средний) — задает порог в 500 регистрации и запросов имен (но умолчанию);
   - **High** (Высокий) — задает порог в 1 000 регистрации и запросов имен;
   - **Custom** (Пользовательский) — позволяет задать порог между 50 и 5 000.
3. Щелкните OK.

Примечание Максимальное число регистрации и запросов имен, которое WINS может принять одновременно, — 25 000. Если этот предел превышен, WINS-сервер прекращает принимать запросы.

Сохранение и восстановление настроек WINS

Задав параметры WINS, вы можете сохранить их, чтобы затем иметь возможность восстановить их на WINS-сервере. Для этого наберите в командной строке:

```
netsh WINS dump >> winsconfig.dmp
```

Здесь winsconfig.dmp — имя сценария настройки, который вы хотите создать. После создания этого сценария вы можете восстановить параметры, набрав:

```
netsh exec winsconfig.dmp
```

Совет Вы также можете использовать этот способ для настройки еще одного WINS-сервера с теми же параметрами: скопируйте сценарий настройки в папку на целевом компьютере и выполните его.

Настройка репликации БД WINS

Вы можете настроить WINS-серверы, чтобы они реплицировали базы друг друга. Тогда БД каждого сервера будут соответствовать текущему состоянию сети и отражать изменения в сети, Способов управления временем выполнения репликации много. Вы также можете выполнить репликацию вручную.

Репликация регулируется заданием ролей извещающих и опрашивающих партнеров. *Извещающий партнер* (push partner) — это WINS-сервер, который уведомляет другие WINS-серверы об изменениях в сети, *опрашивающий* (pull partner) — это WINS-сервер, который запрашивает реплики с извещающего партнера. Вы можете настроить любой WINS-сервер в роли извещающего или опрашивающего партнера или обоих сразу.

Для повышения надежности репликации можно настроить постоянное соединение между партнерами по репликации. При постоянном соединении партнеры сохраняют соединения открытыми, даже когда они простаивают. Это позволяет WINS-серверам быстро и эффективно реплицировать изменения по всей сети.

Настройка стандартных параметров репликации

Перед созданием партнеров по репликации нужно задать параметры по умолчанию. Они используются для настройки новых извещающих и опрашивающих партнеров.

Назначение общих параметров

Общие параметры управляют репликацией и миграцией и задаются так.

1. Раскройте узел сервера, с которым хотите работать, в консоли WINS.
2. Правой кнопкой щелкните в дереве пункт Replication Partners (Партнеры репликации) и выберите Properties.

3. На вкладке General (Общие) пометьте или сбросьте флажок Replicate Only With Partners (Репликация только с партнерами). Если этот флажок спят, вы можете вручную проводить репликацию с любым WINS-сервером в сети.
4. Для не-WINS клиентов в сети создается статическая привязка, которая позволяет зарегистрировать имена их компьютеров в WINS. Если несколько компьютеров могут использовать одни и те же IP-адреса, можно сделать так, чтобы WINS перезаписывал существующие записи информацией о новой регистрации. Для этого выберите Overwrite Unique Static Mappings At This Server (Перезаписывать уникальные статические привязки на этом сервере). Щелкните OK.

Назначение стандартных параметров извещающей репликации

По умолчанию партнеры по репликации настраиваются как для извещающей (push), так и опрашивающей (pull) репликации. Тогда для автоматических обновлений обычно используется не извещающая, а опрашивающая репликация. Также, поскольку партнеры настроены для обоих видов репликации, вы можете запускать извещающую репликацию вручную.

Чтобы извещающая репликация запускалась автоматически или если вы решили изменить стандартные параметры, сделайте так.

1. В консоли WINS раскройте узел сервера, с которым хотите работать.
2. Правой кнопкой щелкните в дереве пункт Replication Partners и выберите Properties.
3. Перейдите на вкладку Push Replication (Извещающая репликация) (рис. 18-5).
4. Извещающая репликация может быть выполнена при запуске WINS и при изменениях адресов. По умолчанию эти параметры не выбраны. Для изменения этого пометьте флажки At Service Startup (При запуске службы), When Address Changes (При изменении адреса) или оба сразу.
5. Параметр Number Of Changes In Version ID Before Replication (Число изменений номера версии до репликации) определяет количество регистрации и изменений, которые должны произойти до того, как опрашивающие партнеры будут извещены, что повлечет репликацию БД. Этот

счетчик накапливает только локальные изменения и не учитывает изменения, присланные другими партнерами. Если данный параметр равен 0, извещающая репликация не выполняется.

6. По умолчанию извещающие партнеры используют постоянные соединения. Если вы этого не хотите, сбросьте флажок Use Persistent Connections For Push Replication Partners (Использовать постоянные соединения для партнеров по извещающей репликации). Щелкните OK.

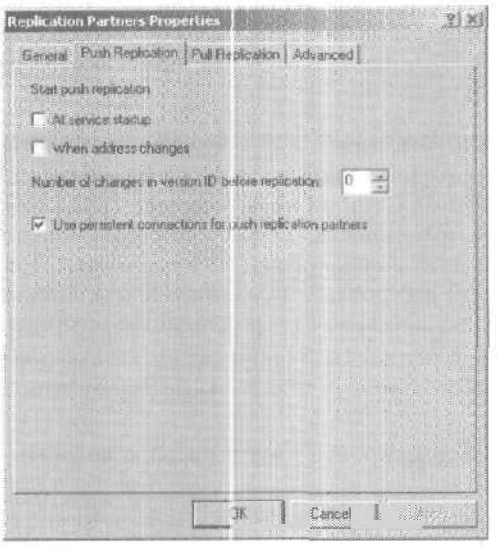


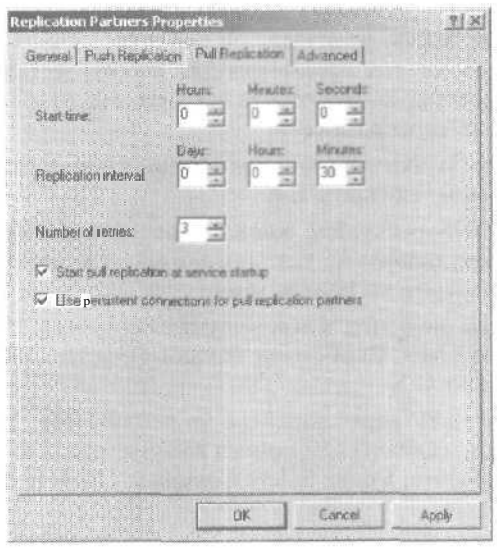
Рис. 18-5. Назначение параметров по умолчанию для управления извещающей репликацией на предприятии.

Назначение стандартных параметров опрашивающей репликации

Опрашивающая репликация — стандартный механизм репликации для партнеров. Поэтому большая часть стандартных параметров опрашивающей репликации включены автоматически. Если вы в первую очередь собираетесь использовать извещающую репликацию, включите автоматический запуск извещающей репликации на вкладке Push Replication и отключите стандартные параметры опрашивающей репликации на вкладке Pull Replication.

Парамегры опрашивающей репликации изменяются так.

1. В консоли WINS раскройте нужный узел сервера.
2. Правой кнопкой щелкните в дереве пункт Replication Partners и выберите Properties.
3. Перейдите на вкладку Pull Replication (Опрашивающая репликация) (рис. 18-6).



Рис, 18-6. Опрашивающая репликация должна использоваться в первую очередь.

4. Параметр Start Time задает время суток, когда начнется репликация, в 24-часовом формате.
5. Параметр Replication Interval задает период запуска репликации, например 30 минут.
6. Параметр Number Of Retries задаст, сколько раз WINS-сервер будет пытаться соединиться с опрашивающим партнером в случае неудачной попытки соединения.
7. По умолчанию опрашивающая репликация запускается при старте WINS-сервера. Для изменения такого поведения снимите флажок Start Pull Replication At Service Startup — опрашивающая репликация будет запускаться только в заданное время.

8. По умолчанию опрашивающие партнеры используют постоянные соединения. Если вы этого не хотите, снимите флажок Use Persistent Connections For Pull Replication Partners и щелкните OK.

Создание извещающих и опрашивающих партнеров

При наличии нескольких WINS-серверов в сети извещающие и опрашивающие партнеры должны выполнять репликацию баз данных WINS. Партнеры по репликации получают стандартные начальные параметры для работы, которые вы настроили для сервера. Настройте репликацию отдельно для каждого WINS-сервера в сети.

Чтобы определить WINS-серверы как извещающие и опрашивающие партнеры, сделайте так,

1. В консоли WINS раскройте запись сервера, с которым хотите работать, одного из тех, для которого будете настраивать партнеров по репликации.
2. Правой кнопкой щелкните в дереве пункт Replication Partners и выберите Now Replication Partner (Создать партнера по репликации).
3. Введите имя или IP-адрес партнера по репликации. Или нажмите Browse (Обзор) для поиска компьютера, с которым нужно работать, в окне Select Computer (Выбор компьютера).
4. Щелкните OK. Если с сервером можно связаться в данный момент, запись о репликации будет создана автоматически со стандартными параметрами. Сервер настраивается, как извещающий и опрашивающий партнер по репликации.

Изменение типа репликации и параметров для партнеров

Стандартные параметры используются для начальной инициализации партнеров по репликации. Эти параметры для каждого партнера всегда можно изменить.

1. В консоли WINS раскройте запись сервера, с которым хотите работать, одного из тех, для которого вы будете настраивать партнеров по репликации.

2. В дереве консоли выберите Replication Partners. На правой панели будут показаны текущие партнеры репликации для данного сервера.
3. Правой кнопкой щелкните запись нужного партнера по репликации и выберите Properties.
4. Перейдите на вкладку Advanced (рис. 18-7).

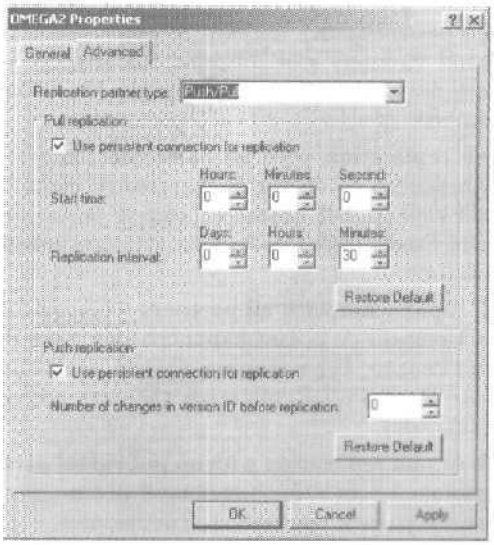


Рис. 18-7. Вы можете изменить стандартные параметры репликации для каждого партнера.

5. Список Replication Partner Type (Тип партнера репликации) показывает, какие типы репликации настроены для этого партнера. По умолчанию большинство клиентов настроены как для извещающей, так и для опрашивающей репликации. Вы можете изменить *это,* выбрав Push или Pull.
6. Остальные параметры такие же, как описанные выше в данной главе. Заметьте, что вы можете настраивать только некоторые параметры в окне Replication Partners Properties.
7. Щелкните OK, когда закончите.

Запуск репликации БД

Иногда может потребоваться сразу обновить БД WINS на партнерах по репликации. Это можно сделать, выполнив немедленную репликацию со всеми партнерами или запустив репликацию между отдельными партнерами. Вы также можете определить тип репликации для выполнения.

- **Forcing replication with all partners** (Выполнение репликации со всеми партнерами): щелкните правой кнопкой папку Replication Partners для сервера, БД которого вы хотите реплицировать, и выберите Replicate Now (Запустить репликацию).
- **Triggering push replication with all partners** (Запуск извещающей репликации со всеми партнерами): щелкните правой кнопкой сервер, БД которого хотите реплицировать, и выберите Start Push Replication (Начать извещающую репликацию).
- **Triggering** pull **replication with all partners** (Запуск опрашивающей репликации со всеми партнерами): щелкните правой кнопкой сервер, БД которого хотите реплицировать, и выберите Stan Pull Replication (Начать опрашивающую репликацию),
- **Triggering push or pull replication with an individual partner** (Запуск извещающей или опрашивающей репликации с отдельными партнерами): выполните следующее.
  1. В консоли WINS щелкните папку Replication Partners для сервера, БД которого хотите реплицировать. Настроенные в данный момент партнеры репликации будут показаны и правой панели.
  2. Щелкните правой кнопкой партнера, с которым хотите реплицировать БД, а затем выберите Start Push Replication или Start Pull Replication.

Управление 5Д WINS

Вы должны активно управлять БД WINS для поддержания работоспособности разрешения имен WINS в сети.

Просмотр привязок в БД WINS

Когда папка Active Registrations (Активные регистрации) выделена в дереве консоли, в правой панели консоли WINS отображены записи, выбранные вами для просмотра. Каж-

дая строка представляет собой запись в БД WINS. В левой части строки вы увидите один или два значка. Значок одного компьютера показывает, что данная привязка — для уникального имени, значок с несколькими компьютерами — что это привязка для группы, домена, Интернет-группы или многоадресной записи. Привязка также показывает:

- **Record** Name (Имя записи) — полное NetBIOS-имя компьютера, группы или службы, зарегистрированных в БД;
- **Type** (Тип) — тип записи, ассоциированный с привязкой, например 00h Workstation;
- **IP Address** — IP-адрес, ассоциированный с привязкой;
- **State** (Состояние) — статус записи, например активная или освобожденная;
- **Static** (Статическая) — метка «X» в этом столбце означает статическую привязку;
- **Owner** (Владелец) — IP-адрес WINS-сервера, владеющего записью;
- **Version** (Версия) — идентификатор версии БД, в которой была создана запись;
- Expiration (Срок действия) — время и дата, когда срок действия привязки истекает; у статической привязки дата истечения действия — Infinite (Не определена), т. е. такая привязка не истекает (кроме случаев, когда она перезаписывается или удаляется).

Очистка БД WINS

Вы должны периодически чистить БД WINS, удаляя старые имена компьютеров. Процесс удаления старых записей из БД запускается автоматически в зависимости от соотношения между интервалом удаления и задержкой удаления, заданными в окне свойств сервера.

Вы также можете запустить очистку вручную. Для этого выберите в консоли WINS сервер, с которым хотите работать, а затем в меню Action — Scavenge Database (Очистить базу данных).

Проверка непротиворечивости БД WINS

В больших сетях с несколькими WINS-серверами БД разных серверов могут иногда рассинхронизироваться друг с другом. Для поддержания целостности можно периодичес-

ки проверять согласованность БД. Существуют два типа такой проверки: проверка непротиворечивости БД и согласованности идентификаторов версии.

Когда вы проверяете непротиворечивость БД, WINS проверяет целостность записей БД на WINS-серверах. Для проверки непротиворечивости выберите в консоли WINS сервер, а затем в меню Action — Verify Database Consistency (Проверить соответствие базы данных).

Когда вы проверяете согласованность идентификаторов версии, WINS сверяет локальные записи с записями на других WINS-серверах, чтобы убедиться в правильности поддерживаемых версий записей. Для проверки согласованности идентификаторов версии выберите в консоли сервер, а затем в меню Action — Verify Version ID Consistency (Проверить соответствие номеров версий).

Автоматическая проверка непротиворечивости БД настраивается так.

1. В консоли WINS щелкните правой кнопкой нужный сервер и выберите Properties.
2. На вкладке Database Verification (Проверка базы данных) выберите Verify Database Consistency Every... (Проверять непротиворечивость базы данных каждые) (рис. 18-8). Затем в соответствующем поле введите интервал времени для проверки, например каждые 24 или 48 часов.
3. В поле Begin Verifying At (Начать проверку в) введите время, когда должна начаться проверка, в 24-часовом формате.
4. Можете задать параметр Maximum Number Of Records Verified Each Period (Максимальное число записей, проверяемых за каждый период); по умолчанию — 30 000.

Примечание Не забудьте, что эта проверка требует много системных и сетевых ресурсов. Для лучшего контроля над временем проведения проверки обычно задают интервал проверки 24 часа, а затем используют поля Begin Verifying At для настройки времени, с которого начнется проверка. Например, еспи вы зададите цикл проверки в 24 часа, а затем введете время начала проверки — 2 часа, 0 минут, 0 секунд, WINS будет проверять БД в 2 часа ночи каждые сутки.

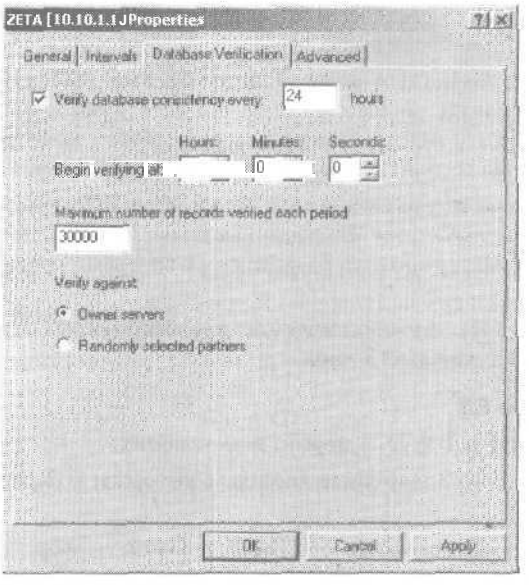


Рис. 18-8. Вместо проверки данных вручную вы можете настроить автоматическую проверку непротиворечивости.

5. Вы можете сверять записи с серверами — владельцами или со случайно выбранными партнерами. Случайный выбор работает лучше, если сеть очень большая и вы не можете проверить все записи за один раз. Иначе выберите пункт Owner Servers (Серверы-владельцы) для проверки записей на серверах, определенных, как владельцы записей.
6. Щелкните OK, когда закончите.

Архивирование и восстановление БД WINS

Администраторы часто забывают о двух задачах WINS-сервера: резервном копировании и восстановлении.

Настройка **WINS для автоматического** резервного копирования

Резервное копирование БД WINS не выполняется по умолчанию, и в случае сбоя вы не сможете ее восстановить. Для защиты БД от сбоев настройте автоматическое резервное копирование или периодически архивируйте ее вручную. Чтобы подготовить WINS к автоматическому резервному копированию, сделайте так.

1. В консоли WINS щелкните правой кнопкой нужный сервер и выберите Properties.
2. На вкладке General в поле Default Backup Path (Путь резервной копии по умолчанию) введите путь к папке, которую хотите использовать для резервного копирования. Вы можете найти такую папку, щелкнув Browse.
3. Для создания резервных копий, даже если WINS-сервер остановлен, выберите Backup Database During Server Shutdown (Архивировать базу данных во время остановки сервера).
4. Щелкните OK. Автоматическое архивирование будет выполняться каждые 3 часа.

Восстановление БД

Рабочую копию БД WINS можно восстановить.

1. В консоли WINS выберите сервер, с которым хотите работать.
2. В меню Action выберите All Tasks, а затем — Stop.
3. В меню Action выберите Restore Database (Восстановить базу данных).
4. В окне Browse For Folder (Обзор папок) выберите подкаталог wins_bak, содержащий наиболее свежую резервную копию, а затем щелкните OK.
5. Если восстановление пройдет удачно, БД WINS вернется в состояние на момент создания копии. В меню Action выберите All Tasks, а затем — Start.
6. Если восстановление не удалось, нам может понадобиться очистить файлы WINS, а затем запустить сервер со свежей БД.

Очистка WINS и запуск со свежей базой данных

Если WINS не восстановится с резервной копии или не запустится нормально, зам может понадобиться очистить все записи и протоколы WINS, а затем запустить сервер со свежей БД.

1. В консоли WINS щелкните правой кнопкой нужный сервер и выберите Properties.

2. На вкладке Advanced найдите и запомните путь к папке из поля Database Path, а затем щелкните OK, чтобы закрыть окно свойств.
3. Остановите **сервер, выбрав в меню** Action **команду** All Tasks, а затем — **Stop.**
4. Используя Проводник, удалите все файлы в папке БД WINS.
5. В консоли WINS правой кнопкой щелкните сервер, который вы восстанавливаете, выберите All Tasks, а затем - Start. WINS-сервер запустится.

Глава 19

Оптимизация DNS

В этой главе обсуждаются методики настройки и управления DNS в сети. DNS - служба разрешения имен, сопоставляющая имена компьютеров IP-адресам. При помощи DNS полное имя узла, например omega.microsoft.com, можно разрешить в IP-адрес, по которому компьютеры находят друг друга. DNS работает через стек протоколов TCP/IP и может интегрироваться с WINS, DHCP и службой каталогов Active Directory. Полная интеграция с этими сетевыми функциями Windows позволяет оптимизировать DNS для доменов Windows 2000.

Понятие DNS

DNS организует группы компьютеров в *домены,* которые для общедоступных сетей организованы в иерархическую структуру на базе Интернета, а для частных сетей — в масштабе предприятия (такие сети называют интрасетями и экстрасетями). Разные уровни внутри иерархии идентифицируют индивидуальные компьютеры, домены организаций и домены верхнего уровня. В полком имени узла omega.microsoft.com, *omega* — имя узла индивидуального компьютера, *Microsoft* — домен организации, а *com* — домен верхнего уровня.

Домены верхнего уровня находятся в корне иерархии DNS и называются *корневыми* (root domains). Они организуются географически, по тинам организации и назначению. Обычные домены типа microsoft.com также называют *родительскими* (parent), так как они — родители организационной структуры. Родительские домены могут состоять из поддоменов, которые могут использоваться для групп или отделов в пределах организации. Поддомены часто называют *дочерними доменами* (daughter domains). Например, полное доменное имя компьютера в отделе кадров может быть

jacob.hr.microsoft.com, где *jacob* — имя узла, *hr* — дочерний домен, а *microsoft.com* — родительский.

Интеграция Active Directory и DNS

Как сказано в главе 5, домены Active Directory используют DNS для реализации своей структуры именования и иерархии. Служба каталогов Active Directory и DNS интегрированы так тесно, что вы должны установить DNS в сети до установки Active Directory.

При установке первого контроллера домена в сети Active Directory у вас будет возможность автоматически установить DNS, если DNS-сервер нельзя найти в сети. Вы также сможете указать, интегрировать ли DNS и Active Directory полиостью. Обычно на оба вопроса отвечают утвердительно. При полной интеграции информация DNS сохраняется прямо в Active Directory, что позволяет задействновать дополнительные возможности Active Directory. Важно отличать частичную и полную интеграцию.

- При частичной интеграции домен хранит данные DNS в обычной файловой системе в текстовых файлах с расширением .DNS. По умолчанию эти файлы находятся к папке %SystemRoot%\System32\Dns. Обновления DNS обрабатываются через единственный полномочный DNS-сервер, назначенный первичным DNS-сервером для конкретного домена или области внутри домена, называемой *зоной*. Клиенты, динамически обновляющие данные DNS средствами DHCP, должны обращаться к первичному DNS-серверу в зоне, иначе их DNS-информация не будет обновлена. Аналогично динамические обновления не пройдут через DHCP, если первичный DNS-сервер недоступен.
- При полной интеграции домен использует интегрированное в каталог хранилище. DNS-информация хранится прямо в Active Directory и доступна через контеинер для объекта dnsZone. Поскольку эти данные — часть Active Directory, любой контроллер домена может получить доступ к ним, а динамическое обновление средствами DHCP можно производить с несколькими хозяевами. Это позволяет любому контроллеру домена, выполняющему службу DNS Server, обрабатывать динамические обновления. Остальные клиенты, динамически обновляющие данные DNS через DHCP, обращаться к любому DNS-ссрверу в

своей зоне. Дополнительное преимущество интеграции каталогов — возможность задействовать систему безопасности каталогов при доступе к DNS-информации.

Рассмотрев способ репликации DNS-информации во всей сети, вы также увидите преимущества полной интеграции с Active Directory. При частичной интеграции DNS-информация хранится и реплицируется отдельно от Active Directory. Имея две отдельные структуры, вы снижаете эффективность работы как DNS, так и Active Directory и усложняете администрирование. Поскольку в DNS изменения реплицируются менее эффективно, чем в Active Directory, наличие двух структур также увеличит сетевой трафик и время репликации изменений DNS во всей сети,

Развертывание DNS *к* сети

Чтобы задействовать DNS в сети, нужно настроить DNS-клиенты и DNS-серверы. Настраивая клиенты, вы задаете IP-адреса DNS-серверов в сети. По этим адресам клиенты могут сообщаться с DNS-серверами из любой точки сети, даже если серверы находятся в других подсетях. Если сеть использует DHCP, нужно настроить DHCP для работы с DNS, задав параметры области DHCP — 006 DNS Servers и 015 DNS Domain Name (см. главу 17).

Кроме того, если компьютеры в сети должны быть доступны из других доменов Active Directory, для них надо создать записи в DNS. Записи DNS организованы в зоны — области внутри домена.

Примечание О настройке DNS-клиента см. главу 15, о настройке DNS-сервера — следующий раздел.

Установка DNS-серверов

Вы можете настроить любой сервер Microsoft Windows 2000 как DNS-сервер одного из четырех типов.

- **Первичный интегрированный в Active Directory — DNS-сервер, полностью интегрированный с Active Directory. Все данные DNS хранятся в каталоге.**
- Первичный сервер — главный DNS-сервер для домена, частично интегрированный в Active Directory, хранит оригинал записей DNS и файлы конфигурации домена в текстовом формате с расширением .DNS.

- Вторичный сервер — DNS-сервер, предоставляющий резервные службы домену, хранит копию записей DNS, полученных от первичного сервера, выполняет обновления путем зонных передач. Вторичные серверы при старте получают данные DNS от первичного сервера и поддерживают их, пока они не будут обновлены или аннулированы.
- Перенаправляющий сервер кэширует DNS-информацию, полученную в результате поиска, и всегда передает запросы другим серверам. Такие серверы хранят данные DNS пока они не будут обновлены или аннулированы или пока не будет перезапущен сервер. В отличие от вторичных перенаправляющие серверы не запрашивает полные копии файлов БД зоны, т. е. когда вы запускаете перенаправляющий сервер, его база пуста.

Перед настройкой DNS-сервера нужно установить службу DNS Server. Позже вы сможете настроить сервер, чтобы он предоставлял интегрированные, первичные, вторичные или перенаправляющие службы DNS.

Установка службы DNS Server

Все контроллеры домена могут выступать в качестве DNS-серверов и в процессе установки контроллера домена вам могут предложить установить и настроить DNS. Если вы ответили утвердительно, значит, DNS уже установлена, а стандартная конфигурация задана автоматически; вам не нужно ничего переустанавливать.

Если вы работаете с рядовым сервером или еще не установили DNS, чтобы установить DNS, сделайте так.

1. Нажмите Start (Пуск), выберите Settings (Параметры), а затем — Control Panel (Панель управления).
2. В Control Panel дважды щелкните Add/Remove Programs (Установка и удаление программ) и нажмите Add/Remove Components (Добавление и удаление компонентов Windows). Вид окна Add/Remove Programs изменится.
3. Под Components щелкните Networking Services (Сетевые службы), а затем — Details (Состав).
4. В открывшемся окне в списке пометьте флажок Domain Name System (DNS).
5. Щелкните OK, а затем — Next. Если спросят, наберите полный путь к файлам дистрибутива Windows 2000 и щелкните Continue (Продолжить).

Теперь служба DNS должна запускаться автоматически при каждой перезагрузке сервера. Если она не запускается, вам придется запускать ее вручную (см. раздел «Пуск и остановка DNS-сервера»).

Настройка первичного DNS-сервера

Каждый домен должен иметь первичный DNS-сервер. Он может быть интегрирован с Active Directory или быть стандартным первичным сервером. Первичные серверы должны иметь зоны прямого и обратного просмотра. Первые служат для разрешения доменных имен в IP-адреса, вторые позволяют подтверждать запросы DNS и решать обратную задачу — сопоставлять IP-адреса доменным именам.

Установив службу DNS Server на сервере, вы можете настроить первичный сервер.

1. Запустите консоль DNS. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и выберите DNS. Появится консоль DNS (рис. 19-1).

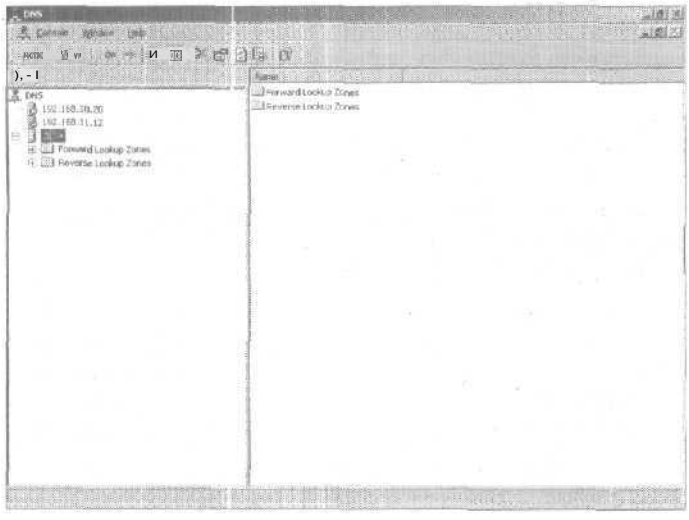


Рис. 19-1. Из консоли DNS управляют DNS-серверами в сети. Как альтернативу консоли DNS можно использовать узел Services And Applications (Службы и приложения) консоли Computer Management (Управление компьютером): раскройте этот узел и щелкните DNS.

2. Если сервер, который вы хотите настроить, не указан в виде дерева, подключитесь к нему. Правой кнопкой щелкните DNS в дереве консоли и выберите Connect To Computer (Соединение с компьютером). Если вы подключаетесь:
   - к локальному серверу, выберите This Computer (Этот компьютер) и щелкните OK;
   - к удаленному серверу, выберите The Following Computer (Следующий компьютер), введите имя или IP-адрес сервера и щелкните OK.
3. Запись для DNS-сервера должна появится в дереве консоли DNS. Правой кнопкой щелкните запись сервера и выберите New Zone (Добавление новой зоны). Запустится мастер создания зоны. Щелкните OK.
4. Теперь вы можете выбрать тип зоны (рис. 19-2). Если *вы* настраиваете первичный сервер, интегрированный в Active Directory, выберите Active Directory-Integrated (Интегрированная в Active Directory) и щелкните Next. Иначе выберите Standard Primary (Основная) и щелкните Next.

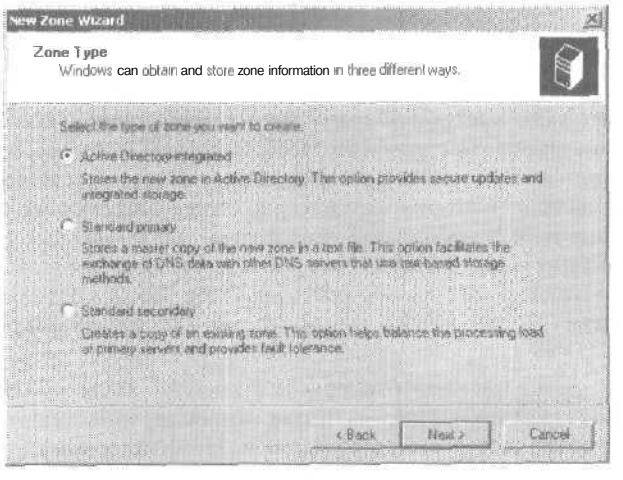


Рис. 19-2. В окне мастера выберите тип зоны.

5. Выберите Forward Lookup Zone (Зона прямого просмотра) и щелкните Next.
6. Введите полное имя DNS для зоны. Это имя определяет, где в иерархии домена DNS будет располагаться сервер

или зона. Например, если вы создаете первичный сервер для домена microsoft.com, наберите имя зоны **microsoft.com.**

7. Если вы настраиваете стандартную первичную зону, задайте имя файла зоны. В соответствующем поле автоматически вводится стандартное имя файла БД для зоны DNS. Вы можете оставить это имя файла или ввести свое.
8. Щелкните Next, а затем — Finish, чтобы завершить процесс. Новая зона добавится к серверу, и основные записи DNS будут созданы автоматически.
9. Один DNS-сервер может обслуживать несколько доменов. Если в сети несколько родительских доменов, например microsoft.com и msn.com, вы можете, повторив этот процесс, настроить другие зоны прямого просмотра. Вам также нужно настроить зоны обратного просмотра (см. раздел «Настройка обратных просмотров»).
10. Создайте дополнительные записи для любых компьютеров, которые должны быть доступны в других доменах DNS (см. раздел «Управление записями DNS»).

Настройка вторичного DNS-сервера

Вторичные серверы предоставляют резервные службы DNS в сети. Если вы используете полную интеграцию с Active Directory, вторичные серверы настраивать не нужно. Вместо этого надо настроить несколько контроллеров домена, чтобы оперировать службами DNS. С другой стороны, если вы используете частичную интеграцию, вам может понадобиться настроить вторичные серверы, чтобы снизить нагрузку на первичный. В небольшой сети в качестве вторичных серверов можно указать имена серверов вашего поставщика услуг Интернета (Internet service provider, ISP), Тогда вы должны обратиться к TSP, чтобы тот настроил для вас вторичные службы DNS.

Поскольку вторичные серверы используют зоны прямого просмотра для большинства типов запросов, зоны обратного просмотра могут не понадобиться. Но файлы зон обратного просмотра нужны для первичных серверов, и они должны быть настроены для корректного разрешения имени домена.

Чтобы создать собственные вторичные серверы для балансировки загрузки и резервирования, сделайте так.

1. Откройте консоль DNS и подключитесь к серверу, который хотите настроить.
2. Щелкните правой кнопкой запись сервера и выберите New Zone.
3. В окне Zone Type (Тип зоны) выберите Standard Secondary (Дополнительная) и щелкните Next.
4. Вторичные серверы могут использовать файлы зоны как прямого, так и обратного просмотра. Сначала создайте зону прямого просмотра, выбрав Forward Lookup Zone и щелкнув Next.
5. Введите имя файла зоны и щелкните Next.
6. Вторичные серверы должны копировать файлы зоны с первичных серверов. Наберите IP-адрес первичного сервера зоны и щелкните Add. Чтобы скопировать данные из других зон, наберите IP-адрес дополнительных серверов.
7. Щелкните Next, а затем — Finish.
8. В загруженной или крупной сети может понадобиться настроить зоны обратного просмотра на вторичных серверах (см. раздел «Настройка обратных просмотров»).

Настройка обратных просмотров

Прямые просмотры нужны для разрешения имен доменов в IP-адреса, а обратные — для разрешения IP-адресов в имена доменов. Каждый сегмент в вашей сети должен иметь зону обратного просмотра. Например, если у вас есть подсети 192.168.10.0, 192.168.11.0 и 192.168.12.0, вы должны иметь три зоны обратного просмотра.

Стандартное правило именования зон обратного просмотра — запись идентификатора сети в обратном порядке и добавление суффикса in-addr.arpa. В предыдущем примере у вас должны получиться зоны 10.168.192.in-addr.arpa, 11.168.192.in-addr.arpa и 12.168.192.in-addr.arpa. Записи в зоне обратного просмотра должны быть синхронизированы с зоной прямого просмотра. При рассинхронизации зон проверка подлинности в домене может дать сбой.

Создать зону обратного просмотра можно так.

1. Запустите консоль DNS и подключитесь к серверу, который хотите настроить.

2. Щелкните правой кнопкой запись сервера и выберите New Zone. Запустится мастер создания зоны. Щелкните Next.
3. Выберите Active Directory-Integrated, Standard Primary или Standard Secondary в зависимости от типа сервера, с которым работаете.
4. Выберите Reverse Lookup Zone и щелкните Next.
5. Наберите идентификатор сети и маску подсети для зоны обратного просмотра. Вводимое значение задает стандартное имя для зоны обратного просмотра.

Совет Если у вас множество подсетей в одной сети, скажем, 192.168.10 и 192.168.11, вводите только сетевую часть для имени зоны, т. е. наберите 168.192.in-addr.arpa и позвольте консоли DNS создать, когда нужно, нужные зоны подсетей.

6. Если вы настраиваете стандартный первичный или вторичный сервер, задайте имя файла зоны. Стандартное имя для файла БД зоны DNS заполняется автоматически. Вы можете использовать это имя файла или ввести свое.
7. Если вы настраиваете вторичный сервер, наберите IP-адрес для первичного сервера зоны и щелкните Add. Если вы хотите скопировать данные из других зон, наберите ГР-адреса дополнительных серверов.
8. Щелкните Next, а затем — Finish.

Настроив зоны обратного просмотра, убедитесь, что они правильно делегируются. Обратитесь в ИТ-отдел организации или к вашему ISP, чтобы проверить, что зоны зарегистрированы в родительском домене.

Управление DNS-серверами

Консоль DNS — удобное средство управления локальными и удаленными DNS-серверами. Основное окно консоли DNS разделено на две панели (рис. 19-3). Левая позволяет получить доступ к DNS-серверам и их зонам, правая — показывает выбранный пункт в развернутом виде.

Бы можете работать с консолью DNS несколькими способами:

- двойной щелчок записи в левой панели раскрывает список файлов для выбранной записи;
- выберите запись в левой панели, чтобы просмотреть в правой панели подробности: состояние зоны, записи домена и т. п.;

- щелкните правой кнопкой запись, чтобы отобразить контекстное меню с доступными командами.

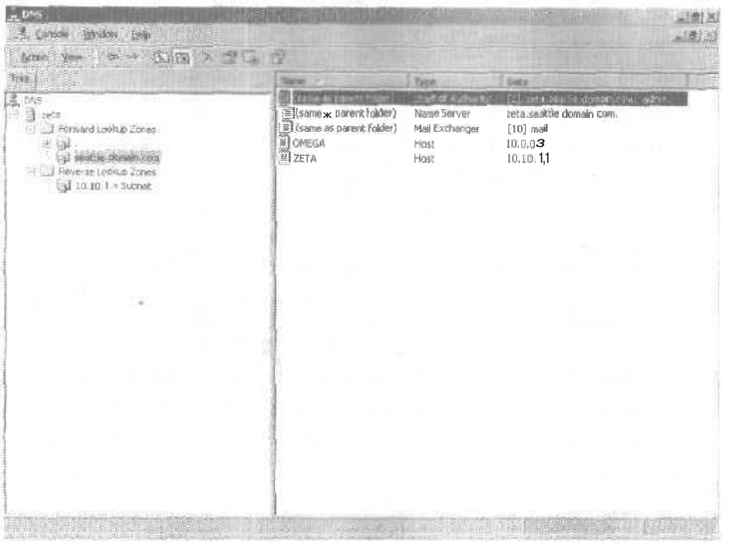


Рис. 19-3. Управляйте доменами и подсетями через палки Forward Lookup Zones и Reverse Lookup Zones.

Папки Forward Lookup Zones и Reverse Lookup Zones предоставляют доступ к доменам и подсетям, настроенным для использования на этом сервере. Выбирая папки домена или подсети в левой панели, вы можете управлять записями DNS для домена или подсети.

Добавление удаленных серверов в консоль DNS

1. Щелкните правой кнопкой DNS в дереве консоли и выберите Connect To Computer, чтобы открыть диалоговое окно (рис. 19-4).
2. Если вы подключаетесь к локальному компьютеру, выберите This Computer. Иначе выберите The Following Computer и наберите IP-адрес или полное имя узла удаленного компьютера, к которому хотите подключиться.
3. Щелкните OK. Если подключение удалось, запись сервера появится в консоли.

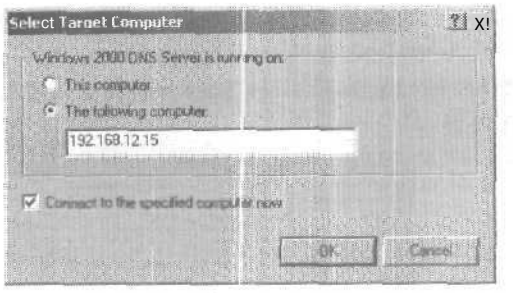


Рис. 19-4. Подключение к локальному или удаленному серверу через диалоговое окно Select Target Computer.

Примечание Если сервер автономный или недоступен из-за ограничений безопасности или проблем со службой удаленного вызова процедур (RPC), подключение не удастся. Однако вы можете добавить сервер к консоли, щелкнув Yes в ответ на запрос.

Удаление сервера из консоли DNS

В консоли DNS можно удалить сервер, выбрав его запись, нажав клавишу DEL и щелкнув OK, чтобы подтвердить удаление. При этом сервер удаляется только из списка серверов; фактически он *не* удаляется из сети.

Пуск и остановка DNS-сервера

Служба DNS Server позволяет управлять DNS-сёраерами. Вы можете запустить, остановить, приостановить и возобновить ее работу из узла Services (Службы) консоли Computer Management или из командной строки. Вы можете также управлять этой службой из консоли DNS. Щелкните правой кнопкой нужный сервер, выберите All Tasks (Все задачи), а затем — Start, Stop, Pause, Resume или Restart.

Примечание В консоли Computer Management щелкните правой кнопкой DNS, выберите All Tasks, а затем — Start, Stop, **Pause,** Resume или Restart.

Создание дочерних доменов в зонах

Из консоли DNS можно создать дочерний домен в зоне. Например, если вы создали первичную зону microsoft.com,

вы могли бы создать в ней поддомены hr.microsoft.com и mis.microsoft.com. Дочерние домены создаются так.

1. В консоли DNS раскройте папку Forward Lookup Zones для нужного вам сервера.
2. Щелкнув правой кнопкой запись родительского домена, выберите New Domain.
3. Введите имя нового домена и щелкните OK. Для hr.microsoft.com введите **hr**, а для mis.microsoft.com — mis.

Создание дочерних доменов в отдельных зонах

По мере роста организации вам может понадобиться разделить пространство имен DNS на зоны. В корпоративной штабквартире вы могли бы определить зону для родительского домена microsoft.com, в филиалах — зоны для каждого офиса, например, memphis.microsoft.com, newyork.microsoft.com и la.microsoft.com.

Дочерний домен создается так.

1. Установите DNS-сервер э каждом дочернем домене и создайте зоны прямого и обратного просмотра для дочернего домена (см. раздел «Установка DNS-серверов»).
2. На полномочном сервере DNS для родительского домена делегируйте полномочия каждому дочернему домену, чтобы дочерние домены могли разрешать и отвечать на DNS-запросы от компьютеров внутри и за пределами локальной подсети.

Полномочия дочернему домену делегируются так.

1. В консоли DNS раскройте папку Forward Lookup Zones для сервера, с которым хотите работать.
2. Щелкните правой кнопкой запись родительского домена и выберите New Delegation. Запустится мастер делегирования.
3. Наберите имя дочернего домена и щелкните кнопку Next (рис. 19-5). Вводимое нами имя обновляет значение в поле Fully Qualified Domain Name (Полное имя домена).
4. Щелкните Add, чтобы открыть диалоговое окно (рис. 19-6).
5. В поле Server Name (Имя сервера) наберите полное имя узла DNS-сервера для дочернего домена.

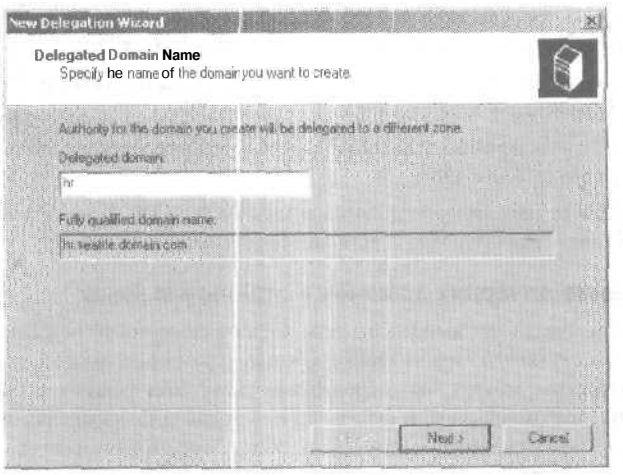
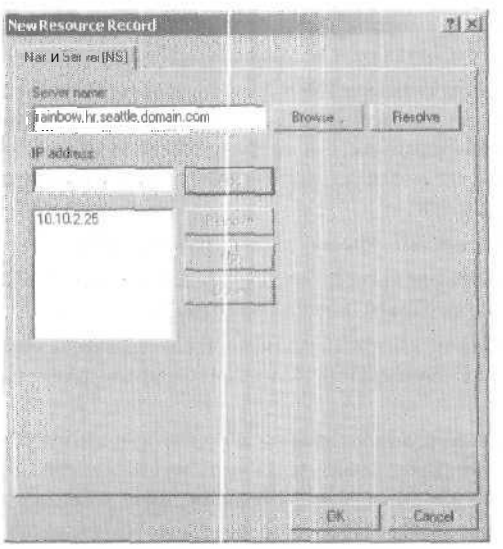


Рис. 19-5. Ввод имени дочернего домена задает полное доменное имя.



РисС. 19-6. Наберите полное доменное имя DNS-сервера для дочернего домена, а затем — IP-адрес(а) для сервера.

6. В поле IP Address (IP-адрес) наберите первичный IP-адрес для сервера. Щелкните Add. Повторите этот процесс,

чтобы задать дополнительные IP-адреса для сервера. Порядок записей определяет приоритет использования IP-адресов; его можно изменить кнопками Up и Down.

Совет Если вы знаете имя сервера, а не его IP-адрес, введите имя в поле Server Name и щелкните Resolve (Сопоставить): IP-адрес отобразится в поле IP Address. Добавьте сервер, щелкнув Add.

7. Щелкните OK и повторите пп. 3-5, чтобы определить другие полномочные DNS-серверы для дочернего домена.
8. Щелкните Next, а затем — Finish, чтобы завершить процесс.

Удаление домена или подсети

1. В консоли DNS щелкните правой кнопкой запись домена или подсети.
2. Выберите Delete (Удалить) и подтвердите действие, щелкнув OK.

Примечание Удаление домена или подсети удаляет все записи DNS в файле зоны, но фактически не удаляет файл зоны на стандартном первичном или стандартном вторичном сервере. Файл зоны остается в папке %SystemRoot%/System32/Dns. Если хотите, можете удалить его.

Управление записями DNS

Создав файлы зоны, к зонам можно добавить записи. Компьютеры, доступные из Active Directory и доменов DNS, должны иметь записи DNS. Типов записей DNS множество, но большинство обычно не используют, так что мы сосредоточимся на тех, что *вам понадобятся.*

- A (адрес) — проецирует ими узла на IP-адрес. Сколько в компьютере сетевых адаптеров или IP-адресов, столько у него будет и записей адресов.
- **CNAME** (каноническое имя) — задает псевдоним для имени узла. Например, запись позволит zeta.microsoft.com получить псевдоним www.microsoft.com.
- MX (обмен почтой) — определяет почтовый сервер для домена, куда будет доставляться почта.
- NS (сервер имен) — указывает сервер имен для домена, обеспечивающий поиск по DNS в разных зонах. Каждый

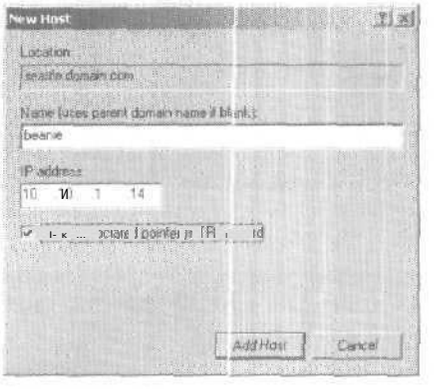
первичный и вторичный сервер имен должен быть объявлен такой записью.

- PTR (указатель) — создает указатель, проецирующий IP-адреса на имя узла для обратного просмотра,
- SOA (начальная запись зоны) — описывает самый полномочный узел зоны, являющийся наилучшим источником данных DNS для зоны. Каждый файл зоны должен содержать SOA-запись (создается автоматически при добавлении зоны).

Добавление записей адреса и указателя

A-запись проецирует имя узла на IP-адрес, а PTR-запись создает указатель на узел для обратного просмотра. Вы можете создать записи адреса и указателя одновременно или по отдельности.

1. В консоли DNS раскройте папку Forward Lookup Zones для нужного вам сервера.
2. Щелкнув правой кнопкой домен, который хотите обновить, выберите New Host (Создать узел). Появится диалоговое окно (рис. 19-7).



Рис, 19-7. Параллельное создание записей A и PTR командой New Host.

3. Наберите имя компьютера без пробелов и IP-адрес.
4. Пометьте флажок Create Associated Pointer (PTR) Record (Создать соответствующую PTR-запись).
5. Щелкните OK.

Примечание Вы можете создать только PTR-записи, если доступна соответствующая зона обратного просмотра (см. раздел «Настройка обратных просмотров»).

6. Щелкните Add Host (Добавить узел). Повторите для добавления других узлов.
7. Кончив, щелкните Done (Готово).

Последующее **добавление** PTR-записи

1. В консоли DNS раскройте папку Reverse Lookup Zones для нужного вам сервера.
2. Щелкнув правой кнопкой подсеть, которую хотите обновить, выберите New Pointer (Создать указатель) (рис. 19-8).

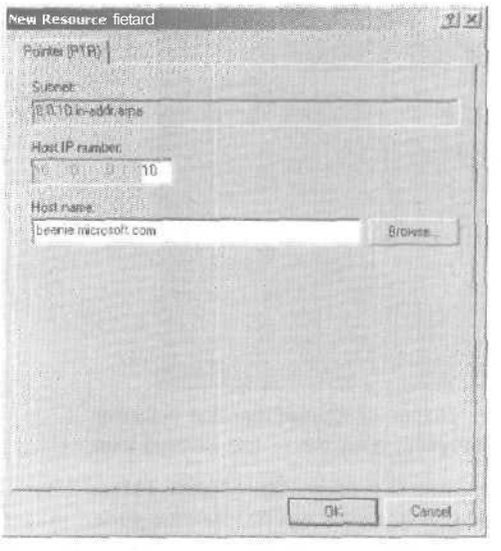


Рис. 19-8. Вы можете добавить PTR-записи позже из окна New Resource Record.

3. Наберите IP-адрес узла и полное доменное имя компьютера, например 10.10.1.14 и heanie.microsoft.com. Щелкните OK.

Добавление псевдонимов DNS с записями CNAME

Псевдонимы узла задаются в CNAME-записях. Псевдонимы позволяют компьютеру представляться многоадресным. На-

пример, узел gamma.microsoft.com **можно** представить **как** www.microsoft.com **и ftp.microsoft.com.**

CNAME-запись создается так.

1. В консоли DNS откройте палку Forward Lookup Zones для нужного вам сервера.
2. Щелкнув правой кнопкой домен, который хотите обновить, выберите New Alias (рис. 19-9).

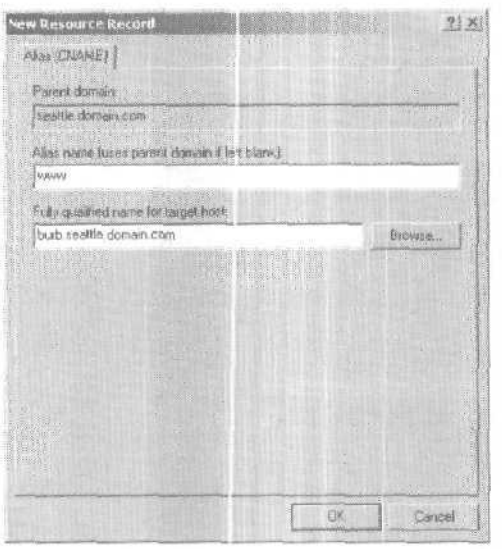


Рис. 19-9. При создании CNAME-записи укажите одночастное имя узла, а затем — его полное имя.

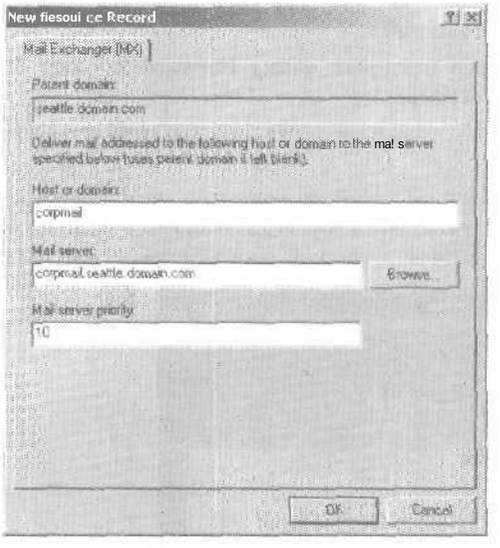
3. Наберите псевдоним в поле Alias Name (Имя псевдонима). Псевдоним — одна из частей имени узла, например www или ftp.
4. В поле Fully Qualified Name For Target Host (Полное имя конечного узла), наберите полное имя узла компьютера, для которого должен быть использован псевдоним.
5. Щелкните OK.

Добавление почтовых серверов

MX-записи задают почтовые серверы для домена. Эти серверы отвечают за обработку или пересылку почты в домене, При создании MX-записи нужно определить приоритет поч-

тоиого сервера в диапазоне 0-65 535. Почтовый сервер с самым низким номером имеет самый высокий приоритет и первым получаст почту. Если почту не удается доставить, ее пытается получить почтовый сервер со следующим номером. MX-запись создается так.

1. В консоли DNS, откройте папку Forward Lookup Zones нужного вам сервера.
2. Щелкнув правой кнопкой домен, который хотите обновить, выберите New Mail Exchanger (Создать почтовый обменник) (рис. 19-10).



Рис, 19-10. Почтовые серверы с самым низким номером имеют самый высокий приоритет.

3. Теперь вы можете создать запись для почтового сервера, заполнив поля:
   - **Host Or Domain** (Узел или домен) — произвольное имя узла;
   - **Mail Server** (Почтовый сервер) — полное имя узла;
   - **Mail Server Priority** (Приоритет почтового сервера) — приоритет узла от 0 до 65 535.

Совет Назначайте номера, чтобы оставалось место для дальнейшего роста. Скажем, введите 10 для почтового сервера с самым высоким приоритетом, 20 — для следующего и т. д.

4. Щелкните OK.

Добавление серверов имен

Записи NS определяют серверы имен для домена. Каждый первичный и вторичный сервер имен должен иметь такую запись. Если ваша сеть обслуживается вторичными службами ISP, не забудьте добавить соответствующие записи NS.

Запись **NS** создается так.

1. В консоли DNS откройте папку Forward Lookup Zones нужного вам сервера.
2. Выберите папку домена в дереве, чтобы просмотреть его записи DNS.
3. Щелкнув правой кнопкой имеющуюся запись NS в панели просмотра, выберите Properties. Появится окно свойств домена с выбранной вкладкой Name Servers (рис. 19-11).

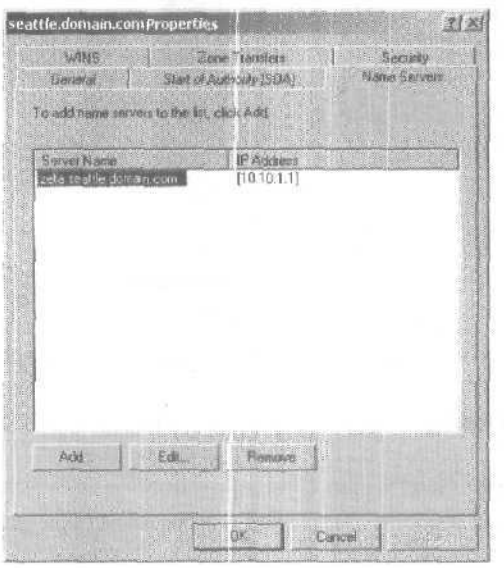


Рис. 19-11. Настройте серверы имен в окне свойств домена.

4. Щелкните Add.
5. В поле Server Name наберите полное имя узла добавляемого DNS-сервера.
6. В поле IP Address введите основной IP-адрес сервера. Щелкните Add. Повторив эту операцию, укажите дополнительные IP-адреса для сервера. Порядок записей определяет IP-адрес, используемый первым. Порядок позволяют изменить кнопки Up и Down.
7. Щелкните OK. Повторите пп. 5-7, чтобы указать другие DNS-серверы для домена.

Просмотр и обновление записей DNS

1. Дважды щелкните нужную зону. Записи для зоны отобразятся в правой панели.
2. Дважды щелкните запись DNS, которую хотите просмотреть или обновить. В открывшемся окне сделайте нужные изменения и щелкните OK.

Обновление свойств зоны и записи SOA

Отдельные свойства зоны можно настроить. Эти свойства задают основные параметры зоны с помощью начальной записи зоны (SOA), уведомления об изменении и интеграции WINS. В консоли DNS свойства зоны настраиваются так.

1. Щелкните правой кнопкой обновляемую зону и выберите Properties.
2. Выберите зону, а затем в меню Action — команду Properties.

Окна свойств для зон прямого и обратного просмотра идентичны, кроме вкладок WINS и WIXS-R. Для зон прямого просмотра отображается вкладка WINS, позволяющая настроить поиск NetBIOS-имен компьютеров, для зон обратного просмотра — вкладка WINS-R, позволяющая настроить обратный просмотр для NetBIOS-имен компьютеров.

Модификация записи SOA

Начальная запись зоны (start of authority, SOA) назначает полномочный сервер имен для зоны и задает основные свойства зоны, например интервалы повтора и обновления. Вы можете изменить эту информацию так.

1. В консоли DNS щелкните правой кнопкой обновляемую зону и выберите Properties.

2. Щелкните вкладку Start Of Authority (SOA) и обновите параметры (рис. 19-12).

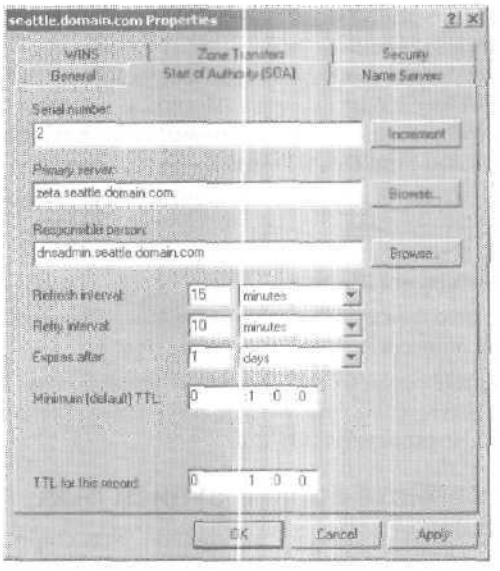


Рис. 19-12. В окне свойств зоны можно задать общие свойства для зоны и обновить запись SOA.

Бы используете следующие поля вкладки Start Of Authority (SOA).

- Serial Number (Серийный номер) — серийный номер, указывающий версию файлов БД DNS. Обновляется автоматически при любом изменении файлов зоны. Вы можете, однако, обновлять этот номер вручную. Его используют вторичные серверы для установления факта изменения записей зон. Если серийный номер первичного сервера *больше* серийного номера вторичного, записи изменились, и вторичный сервер может запросить обновленные записи для зоны. Вы также можете настроить DNS, чтобы уведомлять вторичные серверы об изменениях (это ускорит процесс обновления).
- Primary Server (Основной сервер) — полное доменное имя для *сервера* имен, *заканчивающееся* тонкой. Точка позволяет ограничить имя и гарантировать, что доменная информация не добавляется к записи.

- **Responsible Person** (Ответственное лицо) — электронной адрес сотрудника, ответственного за домен. По умолчанию это *администратор с* точкой в конце, т. е. *администратор@ваш_домен.* При изменении записи поставьте точку вместо символа at (@) в адресе электронной почты и закончите адрес точкой.
- **Refresh** Interval (Интервал обновления) — интервал, в течение которого вторичный сервер проверяет обновления зон. Если он равен 60 минутам, изменения NS-записи могут не передаваться вторичному серверу час. Увеличивая это значение, вы уменьшаете сетевой трафик.
- Retry **Interval** (Интервал повтора) — время ожидания вторичного сервера после неудачной попытки загрузки БД зоны. Если он равен 10 минутам и передача БД зоны не удалась, вторичный сервер прождет 10 минут, прежде чем снова запросит БД зоны.
- **Expires After** (Срок истекает после) — период, в течение которого информация зоны на вторичном сервере действительна. Если за это время вторичный сервер не загрузит данные с первичного, то аннулирует данные в своем кэше и перестанет отвечать на запросы DNS. Если задано 7 дней, данные на вторичном сервере будут доступны 7 суток.
- **Minimum (Default) TTL** (Минимальный срок жизни) - минимальное время жизни кэшированных записей на вторичном сервере в формате дни : часы : минуты : секунды. По достижении этого значения вторичный сервер аннулирует связанную запись и отбрасывает ее. Следующий запрос этой записи должен быть отправлен первичному серверу для разрешения имени. Чтобы сократить трафик в сети и повысить эффективность, задайте большое значение, например 24 часа. Впрочем, учтите, что это замедлит распространение обновлений через Интернет.
- **TTL For This Record** (Срок жизни этой записи) — время жизни самой SOA-записи в формате дни : часы : минуты : секунды. Как правило, должно совпадать с минимальным временем жизни обычных записей.

Уведомление вторичных серверов об изменениях

Свойства зоны, задаваемые на начальной записи, контролируют распространение DNS-информации в сети. Вы также

можете указать, что первичный сервер должен уведомлять вторичные серверы имен об изменениях в БД зоны.

1. В консоли DNS щелкните правой кнопкой обновляемый домен/подсеть и выберите Properties.
2. На вкладке Zone Transfers (Передачи зон) щелкните Notify (Уведомить). Появится диалоговое окно (рис. 19-13):

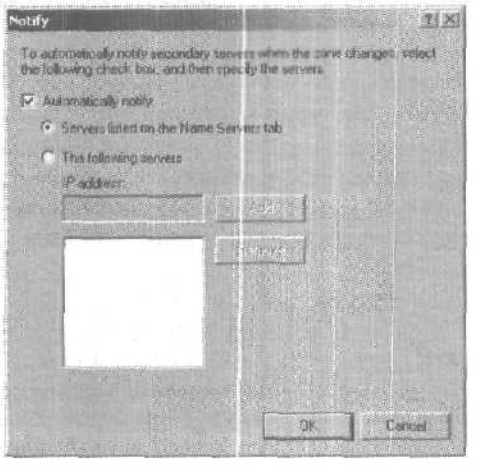


Рис. 19-13. Вы можете уведомить все вторичные серверы, перечисленные на вкладке Name Servers, или указанные серверы.

3. По умолчанию все вторичные серверы, перечисленные на вкладке, уведомляются об изменениях. Если вы хотите указать определенные серверы, выберите The Following Servers и наберите IP-адреса вторичных серверов. Щелкните OK.

Ограничение зонных передач

Ограничение доступа к информации зоны — обычная мера предосторожности. Когда вы ограничиваете доступ к информации зоны, запросить обновления с первичного сервера зоны могут только указанные вами серверы. Это позволяет пропускать запросы через выбранные группы вторичных серверов, например вторичные серверы имен вашего ISP, и скрывать подробности внутренней сети от внешнего мира.

Чтобы ограничить доступ к БД первичной зоны, сделайте так.

1. В консоли DNS правой кнопкой щелкните обновляемый домен/подсеть и выберите Properties.
2. Щелкните вкладку Zone Transfers. Зонные передачи отправляют копию информации зоны другим DNS-серверам, которые могут быть в том же домене или в других доменах. По умолчанию информация зоны передается любому серверу, который ее запросит.
3. Чтобы ограничить передачи серверами имен с вкладки Name Servers, выберите Allow Zone Transfers (Разрешить передачи зон) и щелкните Only To Servers Listed On The Name Servers Tab (Только серверам на вкладке «Серверы имен»).
4. Чтобы ограничить передачи определенными серверами, выберите Allow Zone Transfers и щелкните Only To The Following Servers (Только следующим серверам). Щелкните OK.

Настройка типа зоны

1. В консоли DNS щелкните правой кнопкой обновляемый домен/подсеть и выберите Properties.
2. На вкладке General (Общие) щелкните Change (Изменить). В окне Change Zone Type (Изменение типа зоны) выберите новый тип зоны.

Включение и выключение динамических обновлений

Динамические обновления позволяют клиентам DNS регистрировать и поддерживать собственный адрес и записи указателей. Это полезно для компьютеров, динамически настраиваемых средствами DHCP. Динамические обновления облегчают динамически настраиваемым компьютерам поиск друг друга в сети. Если зона интегрирована с Active Directory вы можете включить безопасные обновления. Тогда динамически обновлять DNS смогут лишь компьютеры и пользователи из списка управления доступом.

Динамические обновления включаются/выключаются так.

1. В консоли DNS щелкните правой кнопкой обновляемый домен/подсеть и выберите Properties.

2. Используйте следующие значения списка Allow Dynamic Updates (Динамическое обновление), чтобы включить/выключить динамические обновления:
   - No — выключить динамические обновления;
   - Yes — включить динамические обновления;
   - Only Secure Updates (Только безопасные обновления) — включает динамические обновления через механизм безопасности Active Directory; доступно только при интеграции с Active Directory,
3. Щелкните OK.

Примечание Параметры интеграции DNS должны также быть настроены для DHCP (см. главу 17).

Управление конфигурацией и безопасностью DNS-сервера

Для управления общей конфигурацией DNS-серверов служит окно свойств сервера. Отсюда вы можете включать/выключать IP-адреса для сервера и управлять доступом к DNS-серверам извне организации. Вы также можете настроить мониторинг, регистрацию и расширенные параметры.

Включение и выключение IP-адресов для DNS-сервера

По умолчанию многоадресные DNS-серверы отвечают на запросы DNS на всех доступных сетевых адаптерах и настроенных IP-адресах. Из консоли DNS вы можете указать, чтобы сервер отвечал на запросы только по заданным IP-адресам.

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Properties.
2. На вкладке Interfaces (Интерфейсы) выберите Only The Following IP Addresses (Только следующие IP-адреса) и наберите IP-адреса, которые должны отвечать на DNS-запросы (рис. 19-14). Только эти IP-адреса будут использоваться для DNS. Остальные IP-адреса на сервере будут недоступны для DNS.

Управление доступом к DNS-серверам извне организации

Ограничение доступа к информации зоны позволяет указать, какие внутренние и внешние серверы имеют доступ к пер-

вичному серверу. Для внешних серверов это определяет, какие серверы могут обратиться в вашу сеть из внешнего мира. Вы можете также указать, какие DNS-серверы в вашей организации могут иметь доступ к внешним серверам. Для этого нужно настроить перенаправление внутри домена.

В отношении перенаправления DNS-серверы внутри домена могут быть такими.

- **Nonforwarders** (Непересылающие) передавают неразрешимые DNS-запросы указанным перенаправляющим серверам. Эти серверы играют роль клиентов для перенаправляющих серверов.
- **Forwarding-only** (Перенаправляющие) могут только кэшировать ответы и передавать запросы на перенаправляющие серверы. Их также называют *только кэширующими* DNS-серверами.
- **Forwarders** (Пересылающие) получают запросы от непересылающих и перенаправляющих серверов. Они. используют обычные методы связи DNS, чтобы решать запросы и возвращать ответы другим DNS-серверам.

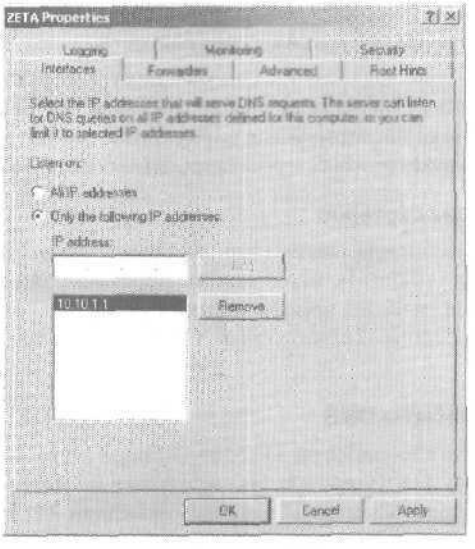


Рис. 19-14, Вкладка Interfaces позволяет указать IP-адресам, что должно управлять запросами и ответами DNS.

Примечание Корневой сервер домена нельзя **настроить** для чистого перенаправления, но все остальные — можно.

Создание непереадресующего DNS-сервера

1. Б консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Properties.
2. На вкладке Forwarders (Пересылка) выберите Enable Forwarders (Разрешить пересылку).
3. Введите IP-адреса пересылающих серверов сети.
4. Укажите Forward Time Out. Это значение контролирует длительность опроса сервера, если тот не откликается. По окончании этого срока опрашивается следующий сервер в списке. Значение по умолчанию — 0 секунд. Щелкните OK.

Создание перенаправляющего сервера

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Properties.
2. На вкладке Forwarders выберите Enable Forwarders, а затем — Operate As Slave Server (Действовать как подчиненный сервер).
3. Введите IP-адреса пересылающих серверов сети.
4. Укажите Forward Time Out. Это значение контролирует длительность опроса сервера, если тот не откликается. По окончании этого срока опрашивается следующий сервер к списке. Значение по умолчанию — 0 секунд. Щелкните OK.

Создание пересылающих серверов

Любой DNS-сервер, не определенный как непересылающий или только перенаправляющий, играет роль пересылающего. Поэтому убедитесь, что на пересылающих серверах *не включены* параметры Enable Forwarders и Operate As Slave Server.

Протоколирование работы DNS

Обычно для наблюдения за работой DNS на сервере используется журнал событий DNS-сервера. Записи этого журнала соответствуют событиям DNS и доступны из узла Event View (Просмотр событий) консоли Computer Management (Управление компьютером). Выявить неполадки DNS поможет вре-

менный журнал отладки, отслеживающий определенные тины событий DNS.

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Properties.
2. На вкладке Logging (рис. 19-15) выберите события, которые хотите временно отслеживать. По умолчанию эти события записываются в файл %SystemRoot%\System32\Dns\Dns.log.

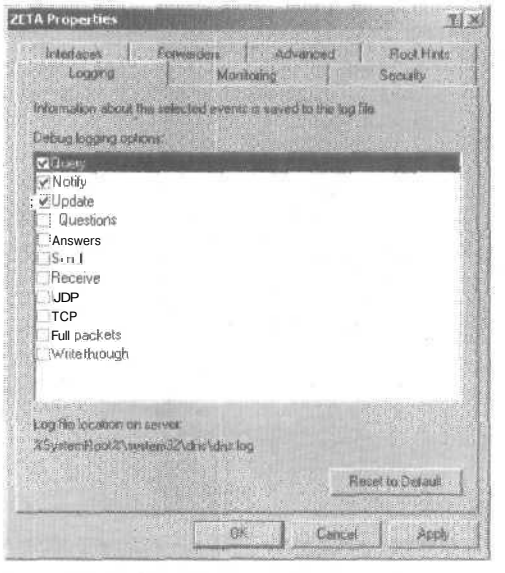


Рис. 19-15. Выберите события, которые хотите регистрировать, и щелкните OK. Не забудьте очистить журнал после отладки.

3. Щелкните OK. По окончании отладки выключите ведение протокола, сбросив любые выбранные ранее флажки на вкладке Logging (Ведение журнала).

Мониторинг DNS-сервера

Windows 2000 имеет встроенные функции мониторинга DNS-сервера. Вы можете вести мониторинг вручную или автоматически.

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Properties.

2. Перейдите на вкладку Monitoring (рис. 19-16). Вы можете выполнить два типа тестов. Чтобы тестировать разрешение имен DNS на текущем сервере, выберите A Simple Query Against This DNS Server (Простой запрос к этому DNS-серверу). Чтобы тестировать разрешение имен DNS в домене, выберите A Recursive Query To Other DNS Servers (Рекурсивный запрос к другим DNS-серверам).

Рис. 19-16. Вы можете настроить DNS-сервер для ручного и автоматического мониторинга. Мониторинг позволяет проверить, что разрешение имен настроено правильно.

3. Вы можете выполнить тест вручную, щелкнув Test Now. или назначить автоматический мониторинг по расписанию, выбрав Perform Automatic Testing At The Following Interval (Выполнить автоматическое тестирование в следующем интервале) и задав интервал в секундах, минутах или часах.

Примечание Если вы активно выявляете неполадки DNS, можете включать тестирование каждые 10-15 секунд, чтобы быстро получить нужные результаты. Если вы проверяете DNS ежедневно, задайте более длинный интервал, например 2-3 часа.

4. Результаты проверки показаны в области Test Results. Вы увидите дату и временную метку, отражающие время выполнения теста и получения результата. Если единственный отказ может быть результатом временного выхода из строя, то несколько отказов обычно свидетельствуют о проблеме разрешения имен DNS.

Интеграция WINS и DNS

Вы можете интегрировать DNS с WINS. Интеграция с WINS позволяет серверу играть роль WINS-сервера или пересылать запросы WINS определенному WINS-серверу. Настроив WINS и DNS для совместной работы, вы можете определить прямой и обратный просмотр по NetBIOS-именам компьютеров, кэширование и значения времени ожидания для разрешения имен W[NS и полную интеграцию с областями NetBIOS.

Настройка поиска WINS в DNS

Когда вы настраиваете поиск WINS в DNS, самая левая часть полного доменного имени может быть разрешена при помощи WINS. Процедура работает так: DNS-сервер ищет запись адреса для полного доменного имени; если запись найдена, сервер применяет ее для разрешения имени, используемого только DNS; иначе сервер выделяет самую левую часть имени и с помощью WINS разрешает имя (как NetBIOS-имя компьютера). Чтобы настроить поиск WINS в DNS, сделайте так.

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Properties.
2. Щелкните вкладку WINS (рис. 19-17).
3. Щелкните Use WINS Forward. Lookup и наберите IP-ад: реса WINS-серверов в сети. Вы должны указать минимум один сервер WINS.
4. Чтобы гарантировать, что запись WINS на этом сервере не реплицируется на другие DNS-серверы в зонных передачах, выберите Do Not Replicate This Record (Не выполнять репликацию этой записи). Это удобно для выявления ошибок и сбоев передачи не-Microsoft DNS-серверу. Щелкните OK.

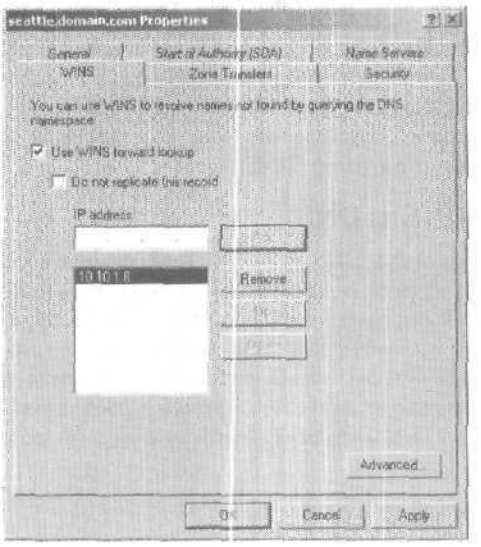


Рис. 19-17. На вкладке WINS настраивается поиск **WINS в DNS.**

Настройка обратного поиска WINS в DNS

Когда настроен обратный поиск WINS в DNS, IP-адрес узла можно разрешить в NetBIOS-имя компьютера. Процедура работает так: DNS-сервер ищет запись указателя ресурса для определенного IP-адреса; если запись найдена, сервер использует ее для разрешения полного доменного имени; иначе сервер отправляет запрос WINS, и но возможности WINS возвращает NetBIOS-имя компьютера для IP-адреса, после чего к этому имени компьютера добавляется домен узла,

Обратный поиск WINS в DNS настраивается так.

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Properties.
2. Перейдите на вкладку WINS-R (рис. 19-18).
3. Выберите Use WINS-R Lookup и, если хотите, — Do Not Replicate This Record. Как и с прямым просмотром, обычно не рекомендуется реплицировать запись WINS-R на не-Microsoft DNS-серверы.

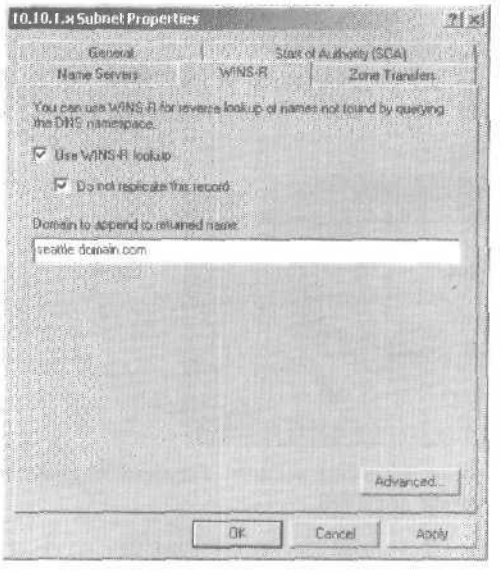


Рис. 19-18. На вкладке WINS-R можно настроить обратный поиск WINS в DNS.

4. В поле Domain To Append To Returned Name (Домен, добавляемый к возвращенному имени) наберите информацию о домене узла. Домен добавляется к имени компьютера, возвращаемому WINS. Например, если вы наберете **seattle.domain.com** и WINS вернет NetBIOS-имя компьютера gamma, DNS-сервер соединит два значения и вернет gamma.seattle.domain.com.
5. Щелкните OK.

Кэширование параметров и значение времени ожидания для WINS в DNS

Интегрируя WINS и DNS, вы должны настроить кэширование и значения времени ожидания для WINS. Параметры кэша определяют, как долго действительны записи, возвращенные WINS. Срок задержки определяет, сколько времени DNS должна ожидать ответа от WINS до истечения таймаута и возвращения ошибки. Эти значения задаются как для прямого, так и обратного поиска WINS.

1. В консоли DNS щелкните правой кнопкой обновляемый домен/подсеть и выберите Properties.
2. Выберите вкладку WINS или WINS-R и щелкните Advanced (Дополнительно). Появится диалоговое окно (рис. 19-19).

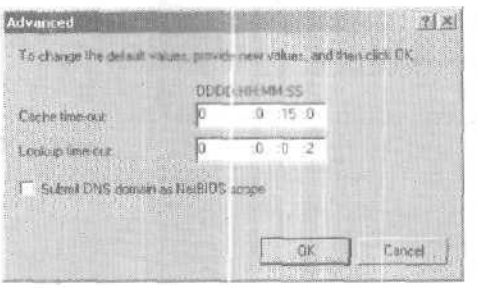


Рис. 19-19. В окне Advanced задайте значения кэширования и времени ожидания для DNS.

3. Задайте значения таймаутов кэширования и времени ожидания в полях Cache Time-Out (Перерыв кэширования) и Lookup Time-Out (Перерыв при поиске). По умолчанию DNS кэширует записи WINS па 15 минут, а время ожидания — 2 секунды. Обычно стоит увеличить эти значения. Попробуйте 60 минут для кэширования и 3 секунды для времени ожидания.
4. Щелкните OK. Повторите этот процесс для других доменов/подсетей.

Настройка полной интеграции с областями NetBIOS

Когда вы настраиваете полную интеграцию, поиск может быть разрешен при помощи NetBIOS-имен компьютеров и областей NetBIOS. Здесь прямой поиск работает так: DNS-сервер ищет запись адреса для полного доменного имени и, если находит, использует ее, чтобы разрешить имя, применяя только DNS; если запись не найдена, сервер извлекает самую левую часть имени как NetBIOS-имя компьютера и остаток имени как область NetBIOS, а затем направляет эти значения WINS для разрешения имени.

Полная интеграция WINS и DNS настраивается так.

1. В консоли DNS щелкните правой кнопкой настраиваемый домен/подсеть и выберите Properties.

2. Выберите вкладку WINS или WINS-R и щелкните Advanced.
3. В окне Advanced выберите Submit DNS Domain As Scope.
4. Щелкните OK. При необходимости повторите этот процесс для других доменов и подсетей.

Перед использованием этой методики убедитесь, что область NetBIOS правильно настроена в сети и что для всех компьютеров в сети применяется согласованная схема именования. Поскольку NetBIOS чувствительна к регистру, запросы разрешаются, только если регистр букв точно совпадает. Учтите также, что для интеграции WINS и DNS, если домен имеет поддомены, поддоменам должны быть делегированы полномочия для служб именования

Предметный указатель

A

Р

С

Об авторе

Уильям Р. Станск (William. R. Stanek, win2000-consulting@tv-press.com) имеет за плечами более 15 лет опыта программирования и разработки. Он один из ведущих экспертов по сетевым технологиям и автор множества известных книг. На протяжении многих лет его практические советы помогали программистам, разработчикам и сетевым инженерам по всему миру. Он также регулярно пишет для ведущих журналов типа «PC Magazine», где его статьи обычно можно найти в разделе «Solutions». Он участвовал в написании более 20 книг, Самые последние из них — «Microsoft Windows 2000. Справочник администратора», «Microsoft Exchange 2000 Server. Справочник администратора», «Microsoft SQL Server 2000. Справочник администратора» и «Windows 2000 Scripting Bible».

Станек активно участвует в разработке коммерческих Интернет-проектов с 1991 г. Первый опыт в области технологий он получил в армии, где прослужил 11 лет. Он обладает обширными знаниями в области разработки серверных решений, шифрования, Интернет-разработки, а также развертывания и технологий электронной коммерции. В 1998 и 1999 гг. Станек занимал пост начальника технической службы iCat (сейчас — часть подразделения Internet Online Services корпорации Intel) *бизнес-подразделения* IDS корпорации Intel. В 1999 и 2000 гг. для компании GeoTrust (Портленд, Орегон) он разработал основополагающие бизнес-стратегии и долгосрочные технологические планы, превратившие компанию из бумажной концепции в многомиллионный бизнес.

Станек имеет степень магистра информационных систем с отличием и степень бакалавра информатики *magna cum laude*. Он гордится своим участием в военной операции и Персидском заливе и был членом экипажа самолета. Совершив множество боевых вылетов в Ирак, он получил девять медалей, включая высшую американскую летную награду — Крест за отличие ВВС США. Сейчас он вместе с женой и детьми проживает на Северо-западном побережье Тихого Океана.

Уильям Р. Станек

Microsoft Windows 2000. Справочникадминистратора

Перевод с английского под общей редакцией *А. В, Иванова*
Переводчики *А. В. Иванов, С. А. Лаврик*
Компьютерная верстка *В, Б. Хильченко*
Технический редактор *Н. Г. Тимченко*
Дизайнер обложки *Е. В. Козлова*

Оригинал-макет выполнен с использованием издательской системы Adobe PageMaker 6.0

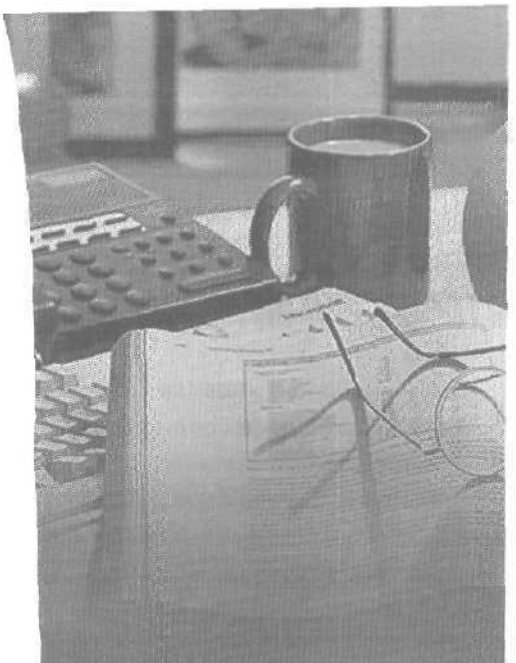
Главный редактор **А. И. Козлов**

Подготовлено к печати издательством «Русская Редакция»
121087, Москва. *ул.* Заречная, д.9
тел.: (095) 142-0571, тел./факс: (ОУ5) 145-4519
e-mail: info@rusedit.ru, http:// www.rusedit.ru

РУССКАЯРЕДАКЦИЯ

Подписано в печать 25.07.02 г. Тираж 1 500 экз.
Формат 84x108/32. Физ. п. л. 18,5

Отпечатано в ОАО «Типография «Новости»
107005, Москва, ул. Фр. Энгельса, 46



Издательство «Русская Редакция» — партнер **Microsoft Press в России** - предлагает **широкий выбор литературы по современным информационным** технологиям.

N РУССКАЯ РЕДАКЦИЯ

тел.: (095) 142-0571; тел./Факс (095) 145-4519;
e-mail: info@rusedit.ru; **http:**//www.rusedit.ru

Наши книги Вы можете приобрести

• **в Москве:**

Специализированный магазин «Компьютерная и деловая книга» Ленинский проспект, строение 38, тел.: (095) 778-7269

«Библио-Глобус» ул. Мясницкая, 6, тел.: (095) 928-3567

«Московский дом книги» ул Новый Арбат, 8, тел.: (095) 290-4507

«Дом технической книги» Ленинский пр-т, 40, тел.: (095) 137-6019

«Молодая гвардия» ул. Большая Полянка, 28, тел (095) 238-5001

«Дом книги на Соколе» Ленинградский пр-т, 73, тел.: (095) 152-4511

"Дом книги на Войковской» Ленинградское ш., 13, стр. 1, тел. (095) 150-6917

«Мир печати» ул. 2-я Тверская-Ямская, 54, тел : (095) 978-5047

Торговый дом книги «Москва» ул. Тверская. 8. тел . (095) 229-6483

• **в Санкт-Петербурге:**

СПб Дом книги, Невский пр-т., 28 тел.: (812) 318-6402

СПб Дом военнвй книги. Невский пр-т., 20 тел.: (812) 312-0563, 314-7184

Магазин «Подписные издания», Литейный пр-т., 57, тел.: (812) 273-5053

Магазин «Техническая книга», ул. Пушкинская. 2, тел.: (812) 164-6565, 164-1413

Магазин «Букволд», Невский пр-т., 13, тел : (812) 312-6734

ЗАО «Торговый Дом «Диалект», тел.: (812) 247-1483

Оптово-розничный магазин «Наука и техника» тел : (812) 567-7025

• **в Екатеринбурге:**

Магазин «Дом книги», ул. Валека. 12, тел.: (3432) 59-4200

• **в Великом Новгороде:**

«Наука и техника», ул. Большая Санкт-Петербургская, 44, Дворец Молодежи, 2-й этаж

• **в Новосибирске:**

000 «Топ-книга», тел.: (3832) 36-1026

» **в Алматы (Казахстан):**

ЧП Болат Амреев, мой. тел.: 8-327-908-28-57, (3272) 76-1404

• **в Киеве (Украина):**

000 Издательство «Ирина-Пресс», тел.: (+1038044) 269-0423

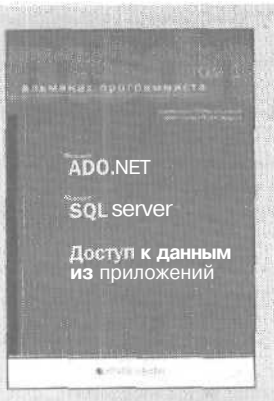
«Техническая книга на Петровке», тел.: (+1038044) 268-5346

Альманах (от араб, аль-манах — календарь) — непериодический сборник, содержащий сведения из различных областей общественной деятельности, обычно с указанием литературных новинок, научных достижений, законодательных изменений и т. д.

Большая Советская Энциклопедия

Представляем
тематический сборник

«АЛЬМАНАХ ПРОГРАММИСТА»



Альманах программиста, том 1; Microsoft ADO.NET, Microsoft SQL Server, доступ к данным из приложений.
400 стр., апрель 2003 г.

Альманах программиста, том 2: Microsoft ASP.NET, Интернет-приложения.
400 стр., сентябрь 2003 г.

Это уникальное издание адресовано профессионалам в области современных информационных технологий. Каждый том представляет собой тематический сборник статей из журнала «MSDN Magazine» и Microsoft MSDN Library по наиболее актуальным и перспективным технологиям разработки программного обеспечения.

Планируется выпуск альманахов по базовым механизмам .NET Framework (модели защиты, отражение, удаленное взаимодействие, сервисы взаимодействия с неуправляемым кодом и т. д.), специфике языков программирования, поддерживающих .NET, отладке/тестированию и другим темам.

Если вас интересует специфическая тематика или определенные материалы из «MSDN Magazine» и MSDN Library, обращайтесь на сайт издательства *www.rusedit.ru* или по адресу *almanah@rusedit.ru*.
Мы постараемся учесть ваши пожелания в будущих выпусках альманаха.

издательство компьютерной литературы

fii РУССКАЯ РЕДАКЦИЯ

Продажа книг
оптом: тел.: (095) 142-0571, e-mail: sale@rusedit.ru;
интернет-магазин: http://www.ITbook.ru, тел.: (095) 145-4519

Microsoft™

Windows 2000

Справочник администратора

Компактный справочник по администрированию Microsoft Windows 2000

Независимо от того, сколько пользователей в вашей организации — 50 или 5 000, этот справочник поможет найти ответы на все, даже самые сложные вопросы администрирования Windows 2000 Server и Windows 2000 Professional. Подробные таблицы,инструкции позволят моментально найти нужную информацию и уменьшить время простоя.

Вы научитесь:

- работать со встроенными средствами администрирования рабочих станций и серверов Windows 2000, просматривать события, оценивать производительность и автоматизировать рутинные процедуры;
- управлять файлами, файловыми системами и дисками; работать с наборами томов и RAID-массивами; обеспечивать общий доступ к данным по сети; архивировать и восстанавливать данные;
- оптимизировать и поддерживать IIS: в книге даны советы по наблюдению, оптимизации и устранению проблем производительности IIS, а также по работе с журналами доступа и сервера;
- работать с доменами Active Directory; выполнять основные задачи в Active Directory; создавать и управлять учетными записями пользователей и групп.

Издательство «Русская Редакция» предствляет новую серию книг Microsoft Press **Справочник администратора** (Administrator's Pocket Consultant)

Каждое издание серии объединяет в себе руководство по эксплуатации и подробный справочник по основным функциям и параметрам системы. Карманный справочник администратора — ваш идеальный помощник в повседневной работе!

ISBN 5-7502-0193-7

9 785750 201938

IT Professional

Web-узел издательства: **www.rusedit.ru**
Интернет-магазин: **www.ITbook.ru**