Учебный
курс
MCSA/MCSE

Сертификационный экзамен 70-215

Microsoft®

Windows 2000 Server

Официальное пособие Microsoft®
для самостоятельной подготовки

Издание 4-е, исправленное

Москва 2003

РУССКАЯ РЕДАКЦИЯ

УДК 004
ББК 32.973.26-018.2
М59

Microsoft Corporation

М59 Microsoft Windows 2000 Server. Учебный курс MCSA/MCSE: Пер. с англ. — 4 -е изд., испр., — М.: Издательско-торговый дом «Русская Редакция», 2003. - 688 стр.: ил.

ISBN 5-7502-0216-X

Данный учебный курс, посвященный Microsoft Windows 2000 Server, поможет освоить способы ручной и автоматической установки, а также настройку параметров этой операционной системы (ОС), В книге кратко описаны различия версий Windows 2000, рассмотрены файловые системы и функции управления дисками. Подробно рассказано об администрировании ОС и службы каталогов Active Directory, сетевых протоколах, маршрутизации, удаленном доступе, новинках системы безопасности, включая протокол Kerberos, мониторинге и оптимизации Windows 2000 Server.

Книга адресована всем, кто хочет получить исчерпывающие знания в области установки, конфигурирования и администрирования Microsoft Windows 2000 Server. Главы книги разбиты на занятия, которые, помимо теоретических сведений, содержат упражнения и контрольные вопросы, которые облегчают освоение материала. Настоящий учебный курс поможет Вам самостоятельно подготовиться к успешной сдаче сертификационного экзамена по программе сертификации Microsoft (Microsoft Certified Systems Engenier, MCSE) № 70-215: Installing, Configuring, and Administering Microsoft Windows 2000 Server,

Богато иллюстрированное издание состоит из 14 глав и предметного указателя. Прилагаемый к книге компакт-диск содержит демонстрационные файлы, словарь терминов и др. справочные материалы.

УДК 004
ББК 32.973.26-018.2

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

ISBN 1-57231-903-8 (англ.)
ISBN 5-7502-0216-X

Содержание

06 этой книге

Мы рады представить Вам учебный курс MSCE по Microsoft Windows 2000 Server. Он поможет Вам освоить ручную и автоматическую установку, а также способы настройки Microsoft Windows 2000 Server. В книге кратко описаны различия версий Windows 2000 и рассмотрены файловые системы и функции управления дисками Windows 2000 Server, подробно обсуждаются администрирование операционной системы и службы каталогов Active Directory, сетевые протоколы, маршрутизация, удаленный доступ и прочие функции прикладного сервера. Кроме того, рассказывается о мониторинге и оптимизации Windows 2000 Server.

Примечание Дополнительную информацию о программе сертификации специалистов Microsoft Certified Systems Engineer см. далее в разделе «Программа сертификации специалистов Microsoft».

Главы учебника состоят из занятий, большинство которых содержат упражнения, предназначенные для демонстрации излагаемых методов и приобретения практических навыков. Каждое занятие заканчивается кратким обобщением материала, а глава — вопросами, которые помогут Вам контролировать уровень своих знаний и усвоения материала.

В разделе *«С* чего начать» вводной главы перечислены аппаратные и программные требования, а также параметры сетевой конфигурации, необходимые для выполнения занятий и упражнений курса. Внимательно прочитайте его, прежде чем изучать материал.

Кому адресована эта книга

Данный курс предназначен для профессионалов в области информационных технологий, которым надо устанавливать, настраивать и сопровождать Windows 2000 Server, или желающих сдать сертификационный экзамен 70-215: Installing, Configuring, and Administering Microsoft Windows 2000 Server.

Для изучения данного курса необходимо:

- знать основы современных сетевых технологий;
- уметь работать с пользовательским интерфейсом ОС Windows (желательно — Windows 95, Windows 98, Windows NT или Windows 2000);
- иметь опыт установки, конфигурирования и поддержки сетей или знать материал в объеме сертификационного экзамена № 70-058 *Networking Essentials (Компьютерные сети. Учебный курс. Второе издание с учетом Microsoft Windows NT 4.0.* Пер. с англ. - М.: «Русская Редакция», 1999);
- иметь опыт работы с основными внутренними и внешними командами операционной системы (cd, dir, fdisk, format и др. I;
- иметь опыт работы с BIOS компьютера;
- иметь опыт работы с Windows 2000 Professional;
- необязателен, но желателен опыт работы с Windows NT.

Справочные материалы

- Журнал *MCP Magazine Online* (http://www.mcpmag.com).
- Web-узел Microsoft (http://www.microsoft.com) и ежемесячный электронный журнал *Microsoft TechNet Technical Plus*, доступный на компакт-лисках и на Web-узле Microsoft.
- *Microsoft Windows 2000 Server Resource Kit.* Microsoft Press, 1999.
- *MSCE Training Kit — Microsoft Windows 2000 Professional.* Microsoft Press, 2000.
- *Компьютерные сети. Учебный курс. 2-е издание сучетом Microsoft Windows NT 4.0.* Пер. с англ. — М.: «Русская Редакция», 1999.
- Silberschatz A and P. Galvin. *Operating System Concepts,* 5th ed. Addison-Wesley Publishing Company, 1998. Одна из хороших книг, в которых рассматриваются основы ОС.
- Журнал *Windows 2000 Magazine*, изд. компании Duke Communications. Электронную версию журнала см. по адресу http://www.winntmag.com.
- Web-узел Sysinternals Freeware (http://www.sysinternals.com).

Содержимое компакт-диска

Компакт-диск учебного курса содержит ряд вспомогательных средств, нужных при изучении всего курса. Это примеры, файлы для выполнения упражнений и дополнительные статьи по темам занятий, а также словарь терминов и примеры файлов ответов для автоматической установки Windows 2000 Server. С этими документами можно работать прямо с компакт-диска или скопировав их на жесткий диск. Подробности о содержимом и работе с компакт-диском см. в файле README.txt на компакт-диске.

Соглашения, принятые в учебном курсе

Прежде всего Вы должны усвоить терминологию и обозначения, принятые в учебнике, и разобраться в логике построения книги.

Структура книги

- Каждая глава начинается с раздела «В этой главе», содержащего краткий обзор обсуждаемых тем.
- Главы делятся на занятия, большинство из которых включают упражнения. Выполнив их, Вы закрепите изученный материал и приобретете практические навыки. Упражнения состоят из этапов и обозначаются значком на полях.
- Каждую главу завершает раздел «Закрепление материала», вопросы которого помогут проверить, насколько твердо Вы усвоили материал.
- Приложение А содержит вопросы всех глав книги и ответы на них.
- В приложении Б описана установка и администрирование пакетов обновлений в Windows 2000.

Примечания

Практически во всех главах встречаются примечания разных видов:

- Совет — поясняет возможный результат или описывает альтернативный метод решения задачи;
- **Внимание!** — предупреждает Вас о возможной потере данных или содержит сведения, необходимые для выполнения поставленной задачи;
- Примечание — содержит дополнительную информацию.

Обозначения

- Вводимые Вами символы или команды набраны **строчными буквами полужирного начертания.**
- *Курсив* в операторах указывает, что в этом месте Вы должны подставить собственные значения; названия книг также напечатаны *курсивом.*
- Имена файлов, папок и каталогов начинаются с Прописных Букв (за исключением имен, которые Вы задаете сами). Кроме особо оговоренных случаев, для ввода имен файлов и каталогов в диалоговом окне или в командной строке Вы можете использовать строчные буквы.
- Расширения имен файлов набраны строчными буквами.
- Аббревиатуры напечатаны ПРОПИСНЫМИ БУКВАМИ.
- Примеры кода, текста, выводимою на экран и текста, вводимого в командной строке выделены моноширинным шрифтом.
- Необязательные элементы операторов заключены в скобки []. Например, [*имя_файла*] в синтаксисе команды означает, что после команды можно указать имя файла. Сами скобки вводить не надо.
- Значками на полях помечены конкретные разделы.

Значок	Описание
	Файлы на компакт-диске. Некоторые файлы нужны для выполнения упражнений, другие содержат дополнительные материалы по темам занятий. О назначении и расположении рассказывается в сопутствующем тексте.
	Упражнение по закреплению навыков, приобретенных при изучении материала.
	Вопросы, отвечая на которые, Вы проверите, насколько твердо усвоили изложенный материал. Вопросы обычно сгруппированы в конце главы, ответы см. в приложении А «Вопросы и ответы».

Клавиатура

- Знак «+» между названиями клавиш означает, что их следует нажать одновременно. Например, выражение «Нажмите Alt+Tab» обозначает, что нужно нажать клавишу Tab, удерживая нажатой клавишу Alt.
- Запятая между названиями клавиш означает их последовательное нажатие. Например, выражение «Нажмите Alt, F, *X*» означает, что надо последовательно нажать и отпустить указанные клавиши. Если же указано «Нажмите Alt+W, L», то Вам придется сначала нажать клавиши Alt и W вместе, потом отпустить их и нажать клавишу L.
- Команды меню можно выбирать с клавиатуры. Для этого нажмите клавишу Alt (чтобы активизировать меню), а затем последовательно — выделенные или подчеркнутые буквы в названиях нужных Вам разделов меню или команд. Кроме того, некоторым командам сопоставлены клавиатурные сокращения (они указаны в меню).
- Флажки и переключатели также можно устанавливать и снимать с клавиатуры. Для этого достаточно нажать Alt, а затем клавишу, соответствующую подчеркнутой букве в названии флажка или переключателя. Кроме того, нажимая клавишу Tab, Вы можете активизировать нужный параметр, а затем установить или снять выбранный флажок или переключатель, нажав клавишу «пробел».
- Работу с диалоговым окном всегда можно прервать, нажав клавишу ESC.

Обзор глав и приложений

Этот курс, предполагающий самостоятельную работу, включает занятия, упражнения и проверочные вопросы, а также мультимедийные презентации, которые помогут Вам научиться настраивать и обслуживать Windows 2000. Курс рассчитан на последовательное изучение, но не исключена и возможность работы лишь с интересующими Вас главами. Советуем тогда обращать внимание на раздел «Прежде всего» в начале каждой главы, где указаны предварительные требования для выполнения упражнений.

Ниже кратко описаны главы и приложения учебного курса.

- В главе «Об этой книге» собраны сведения о содержании учебника, о структурных единицах и условных обозначениях, принятых в нем. Внимательно прочитайте ее: это поможет Вам эффективнее работать с материалами курса, а также выбрать интересующие Вас темы. Здесь также приводится информация по установке, необходимая для успешного выполнения упражнений.
- В главе 1 «Введение в Windows 2000» рассказано о возможностях Windows 2000, архитектуре операционной системы и службе каталогов Windows 2000.
- В главе 2 «Установка и конфигурирование Microsoft Windows 2000 Server» описаны процедуры подготовки, установки и обновления до Windows 2000, а также устранение неполадок установленной ОС Windows 2000.
- В главе 3 «Автоматическая установка Microsoft Windows 2000 Server» обсуждается подготовка и автоматизация установки Windows 2000 Server и серверных приложений.
- Глава 4 «Файловые системы Microsoft Windows 2000» посвящена управлению жесткими дисками, файловым системам Windows 2000 и их безопасности.
- В главе 5 «Дополнительные файловые системы» описаны распределенная файловая система (DFS) и служба репликации файлов (FRS).
- В главе 6 «Служба каталогов Active Directory» обсуждается планирование, развертывание и администрирование Active Directory.
- Глава 7 «Администрирование Microsoft Windows 2000 Server» посвящена использованию управляющей консоли, администрированию учетных записей пользователей и групп, а также внедрению групповой политики.
- В главе 8 «Администрирование служб печати» рассказано о подсистеме печати Windows 2000 и описана процедура установки, управления и подключения сетевого принтера. Кроме того, обсуждается взаимосвязь службы каталогов Active Directory и подсистемы печати.
- В главе 9 «Сетевые протоколы и службы» рассматриваются сетевые протоколы и подробно рассказывается о TCP/IP, DCHP, WINS и DNS.
- В главе 10 «Служба RRAS» описываются маршрутизация и удаленный доступ, включая установку RAS и VPN, а также использование утилит RRAS.
- В главе 11 «Microsoft Windows 2000 Security» обсуждаются инфраструктура открытых ключей, технологии открытых ключей и протокол Kerberos. Описаны также средства настройки системы защиты и внедрение аудита в Windows 2000.
- В главе 12 «Надежность и доступность» рассказано об управлении аппаратными устройствами и драйверами, о резервном копировании в Windows 2000, о разработке стратегии защиты от непредвиденных происшествий и восстановлении системы после них.
- В главе 13 «Мониторинг и оптимизация» описаны процессы мониторинга и оптимизации производительности Windows 2000. Кроме того, обсуждается SNMP и работа с Performance Console, Network Monitor и Task Manager.
- Глава 14 «Серверы приложений Microsoft Windows 2000» посвящена установке и настройке Internet Information Services 5.0, служб Telnet и Terminal Services.

- В приложении А «Вопросы и ответы» приведены ответы на вопросы из упражнений и разделов «Закрепление материала» всех глав учебного курса.
- В приложении Б «Установка пакетов обновлений» описана установка и администрирование пакетов обновлений в Windows 2000,

С чего начать

Данный курс предназначен для самостоятельного изучения, поэтому Вы можете пропускать некоторые занятия, чтобы вернуться к ним потом. И все же помните, что для выполнения упражнений главы в большинстве случаев надо выполнить упражнения предыдущих глав. Чтобы определить, с чего начать изучение курса, обратитесь к этой таблице:

Если Вы	Что делать
готовитесь к сдаче сертификационного экзамена 70-215: Installing, Configuring and Administering Microsoft Windows 2000 Server	см. раздел «Начало работы», изучите книгу в произвольном порядке.
хотите изучить информацию по определенной теме экзамена	см. раздел «Материалы для подготовки к экзаменам».

Материалы для подготовки к экзаменам

В таблицах перечислены темы сертификационного экзамена 70-215: Installing, Configuring, and Administering Microsoft Windows 2000 Server и главы настоящего учебного курса, где обсуждаются соответствующие вопросы.

Примечание Конкретное содержание любого экзамена определяется компанией Microsoft и может быть изменено без предварительного уведомления.

Установка Windows 2000 Server

Тема	Где обсуждается	
	Глава	Занятие
Ручная установка Windows 2000 Server	2	1-2
Автоматическая установка Windows 2000 Server	3	1-3
• Создание файлов ответов с помощью Setup Manager для автоматизации установки Windows 2000 Server	3	1–3
• Создание и настройка автоматизированных методов установки Windows 2000	3	1-3
Обновление сервера с Microsoft Windows NT 4.0	2	3
Развертывание пакетов обновлений	12	1
Решение проблем при установке	2	4

Установка, настройка и решение проблем доступа к ресурсам

Тема	Где обсуждается	
	Глава	Занятие
Установка и настройка сетевых служб	14	1–4
	9	3–5
Мониторинг, настройка, решение проблем и управление доступом к принтерам	5	2-5
Мониторинг, настройка, решение проблем и управление доступом к файлам, папкам и разделяемым каталогам	4	1-4
	5	1-2
	14	1-2
Настройка, управление и решение проблем в изолированной распределенной файловой системе (DFS)	5	1
Настройка, управление и решение проблем в доменной распределенной файловой системе (DFS)	5	1
	6	3
Мониторинг, настройка, решение проблем и управление локальной безопасностью файлов и папок	4	4
Мониторинг, настройка, решение проблем и управление доступом к файлам и папкам общего каталога	4	4
Мониторинг, настройка, решение проблем и управление доступом к файлам и папкам через службы Web	14	1-2
Мониторинг, настройка, решение проблем и управление доступом к службам Web	14	1-2

Настройка и решение проблем с аппаратными устройствами и драйверами

Тема	Где обсуждается	
	Глава	Занятие
Настройка аппаратных устройств	12	1
Настройка параметров подписывания драйверов	12	1
Обновление драйверов устройств	12	1
Устранение неполадок устройств	12	1

Управление, мониторинг и оптимизация производительности, надежности и доступности системы

Тема	Где обсуждается	
	Глава	Занятие
Мониторинг и оптимизация использования ресурсов системы	13	2-5
Управление процессами	13	5
• Задание приоритета, запуск и останов процессов	13	5
Оптимизация производительности диска	13	1
Управление и оптимизация доступности сведений о состоянии системы и пользовательских данных	12	1, 3
Восстановление системных и пользовательских данных	12	2, 4

(*окончание*)

Тема	Где обсуждается Глава	Занятие
• Восстановление системных и пользовательских данных с помощью утилиты Backup	12	2, 4
• Восстановление системы в безопасном режиме	12	4
• Восстановление системы с помощью Recovery Console	12	4

Управление, настройка и устранение **неполадок** хранилищ

Тема	Где обсуждается Глава	Занятие
Настройка и управление профилями пользователей	7	2
Мониторинг, настройка и решение проблем с дисками и томами	12 13	3 1
Настройка сжатия данных	13	1
Мониторинг и настройка дисковых квот	13	1
Восстановление после отказа диска	12	4

Настройка и устранение неполадок сетевых соединений

Тема	Где обсуждается Глава	Занятие
Установка, настройка и решение проблем совместного доступа	4	4
Установка, настройка и решение проблем с виртуальной частной сетью (VPN)	10	4
Установка, настройка и решение проблем с сетевыми протоколами	9	*1,2*
Установка и настройка сетевых служб	9 13	3-5 4
Настройка, мониторинг и решение проблем с удаленным доступом	10	1–3, 5
• Настройка входящих соединений	10	1-3
• Создание политики удаленного доступа	10	3
• Настройка профиля удаленного доступа	10	1–3
Установка, настройка и решение проблем с Terminal Services	14	4
• Удаленное администрирование серверов с помощью Terminal Services	14	4
• Настройка Terminal Services для совместного использования приложений	14	4
• Настройка приложений для работы с Terminal Services	14	4
Настройка свойств соединения	2 9 10	2 2–5 3, 4
Установка, настройка и решение проблем с сетевыми адаптерами и драйверами	2 9 12	1, 2 2 1

Внедрение, мониторинг и решение проблем безопасности

Тема	Где обсуждается	
	Глава	Занятие
Шифрование данных на диске с помощью EFS	11	2
Внедрение, настройка, управление и решение проблем с локальной и системной политиками в среде Windows 2000	7	4
Внедрение, настройка, управление и решение проблем с аудитом	11	5
Внедрение, настройка, управление и решение проблем с локальными учетными записями	7	2
Внедрение, настройка, управление и решение проблем с политикой учетных записей	7	2, 4
Внедрение, настройка, управление и решение проблем с безопасностью при помощи Security Configuration Tool Set	11	4

Начало работы

Данный курс предназначен для самостоятельного изучения и содержит упражнения и практические рекомендации, которые помогут Вам освоить Windows 2000. Для выполнения части упражнений Вам потребуется сеть из двух компьютеров или подключение к большей сети. Рекомендуется, чтобы сеть, соединяющая компьютеры, не была изолированной. Возможности обоих компьютеров должны быть достаточными для запуска Windows 2000 Server.

Внимание! При выполнении части упражнений потребуется изменить конфигурацию серверов. Если **Вы** подключены к большой сети, это может привести к нежелательным результатам. Перед выполнением таких упражнений предварительно проконсультируйтесь с сетевым администратором.

Первый компьютер будет обозначен как Computer 1 с именем Server01, а второй — как Computer 2 с именем Server02. Возможности обоих компьютеров должны быть достаточными для запуска Windows 2000 Server. Если у Вас лишь один компьютер, изучите текст упражнения и попытайтесь понять предпринимаемые действия. Подробнее о компьютерах Computer I и Computer 2 см. раздел «Подготовка компьютера к выполнению упражнений».

В упражнениях и описаниях процедур для описания процесса перемещения по элементам интерфейса Windows, например по управляющей консоли (MMC), используются раскрывающиеся меню. Кроме того, к большинству объектов интерфейса Windows можно обратиться посредством контекстных меню. Чтобы открыть контекстное меню, наведите указатель мыши на объект и щелкните правой кнопкой.

Аппаратное обеспечение

Компьютер должен соответствовать приведенной ниже минимальной конфигурации, а установленное на нем оборудование необходимо выбрать из списка совместимых устройств Microsoft Windows 2000 Hardware Compatibility List:

- процессор Pentium 133 МГц;
- 64 Мб памяти;

- 2 Гб свободного пространства для загрузочного раздела (раздела, содержащего файлы операционной системы) и прочих файлов, создаваемых при выполнении упражнений курса;
- 550 Мб невыделенного пространства на компьютере Server01 (при выполнении упражнений главы 4 Вы разобьете это пространство на разделы);
- 12-скоростной привод CD-ROM;
- монитор SVGA (рекомендуется разрешение 800x600 или более высокое);
- мышь Microsoft или другое аналогичное устройство;
- модем на первом и втором компьютерах;
- доступ к Интернету (рекомендуется).

Существует несколько способов определить совместимость Вашего оборудования. Можно, например:

- просмотреть файл \Support\Hcl.txt на установочном компакт-диске Windows 2000 Server;
- просмотреть наиболее полный список поддерживаемого оборудования на Web-узле Microsoft Windows Hardware Quality Labs по адресу http://www.microsoft.co/hcl/default.asp;
- при ошибке в URL перейти по адресу http://www.microsoft.com и ввести в строке поиска HCL.

Программное обеспечение

Для выполнения упражнений Вам потребуется следующее ПО:

- установочный компакт-диск Windows 2000 Server;
- Windows 2000 Server (120-дневная пробная версия) и инструкции по загрузке ПО, которые можно найти на Web-узле Microsoft по адресу http://www.microsoft.com/windows/2000/default.asp;
- 32-разрядная ОС Windows (Windows 9x, Windows NT 3.51 или Windows NT 4.0), установленная на втором компьютере.

Подготовка компьютера к выполнению упражнений

Настройте компьютер согласно инструкциям поставщика.

Если в упражнении используется сеть, убедитесь, что компьютеры способны взаимодействовать. Компьютер Computer 1 станет контроллером домена; ему будет присвоено учетное имя ServerOI и доменное имя microsoft.com. ServerOI будет контроллером домена microsoft.com.

Компьютеру Computer 2 будут присвоены учетное имя Server02 и доменное — microsoft.com. В большинстве упражнений компьютер Server02 будет играть роль рядового сервера домена.

Подготовка к изучению курса

Установка Windows 2000 Server является частью данного учебного курса и описана в главах 2 и 3. Чтобы снизить вероятность появления проблем при выполнении упражнений, на компьютерах должно быть установлено только оборудование из списка HCL, компьютеры должны соответствовать минимальным аппаратным требованиям; их надо соединить изолированной сетью. Рекомендуется, чтобы на обоих были установлены жесткие диски емкостью 3 Гб и 128 МБ ОЗУ; кроме того, на них должно быть установлено лишь необходимое для изучения данного курса ПО.

В процессе обучения Вам встретятся переменные среды:

- %systemroot% — указывает на каталог с файлами ОС Windows 2000; обычно %systemroot% соответствует C:\Winnt;
- %windir% — указывает на тот же каталог, что и %systemroot%, и используется в Windows 9x;
- %systemdrive% — указывает на корневой каталог загрузочного диска; например, если Вы установили Windows 2000 в папку C:\Winnt, эта переменная среды указывает на C:\.

Программа сертификации специалистов Microsoft

Программа сертификации специалистов Microsoft (Microsoft Certified Professional, MCP) — отличная возможность подтвердить Ваше знание современных технологий и программных продуктов этой фирмы. Лидер отрасли в области сертификации, Microsoft разработала современные методы тестирования. Экзамены и программы сертификации подтвердят Вашу квалификацию разработчика или специалиста по реализации решений на основе технологий и программных продуктов Microsoft. Сертифицированные Microsoft профессионалы квалифицируются как эксперты и высоко ценятся на рынке труда.

Программа сертификации специалистов предлагает 8 типов сертификации по разным специальностям.

- *Сертифицированный специалист Microsoft (Microsoft Certified Professional, MCP)* — предполагает доскональное знание по крайней мере одной операционной системы Microsoft. Сдав дополнительные экзамены, кандидаты подтвердят свое право на работу с продуктами Microsoft BackOffice, инструментальными средствами или прикладными программами.
- *Сертифицированный специалист Microsoft + Интернет (MCP + Internet)* должен разбираться в планировании систем защиты, установке и конфигурировании серверных продуктов, управлении ресурсами сервера, расширении возможностей сервера средствами сценариев интерфейса общего шлюза (Common Gateway Interface, CGI) и интерфейса прикладного программирования сервера Интернета (Internet Server Application Programming Interface, ISAPI), мониторинге работы сервера, анализе его производительности и устранении неисправностей.
- *Сертифицированный специалист Microsoft + Site Building (MCP + Site Building)* — планирование, создание, поддержка и управление Web-узлами с применением технологий и продуктов Microsoft.
- *Сертифицированный системный инженер Microsoft (Microsoft Certified Systems Engineer,* MCSE) — предполагает умение эффективно планировать, развертывать, сопровождать и поддерживать информационные системы на базе Microsoft Windows 9x, Microsoft Windows NT и интегрированного семейства серверных продуктов Microsoft BackOffice.
- *Сертифицированный системный инженер Microsoft + Интернет (MCSE + Internet)* — развертывание и сопровождение многофункциональных решений для интрасети и Интернета, включая программы просмотра, представительские серверы, базы данных, системы сообщений и коммерческие компоненты. Кроме того, сертифицированные по этой специальности инженеры должны уметь управлять Web-узлом и проводить его анализ.
- *Сертифицированный администратор баз данных Microsoft (Microsoft Certified Database Administrator, MCDBA)* — разработка физической структуры, логических моделей данных, создание физических БД, создание служб доступа к данным с использованием T-SQL, управление и поддержка БД, настройка и управление системой защиты, мониторинг и оптимизация БД, а также установка и настройка Microsoft SQL Server.

- *Сертифицированный разработчик программных решений на основе продуктов Microsoft (Microsoft Certified Solution Developer, MCSD)* — разработка и создание прикладных приложений с применением инструментальных средств, технологий и платформ Microsoft, включая Microsoft Office и Microsoft BackOffice.
- *Сертифицированный преподаватель Microsoft (Microsoft Certified Trainer, MCT)* — теоретическая и практическая подготовка для ведения соответствующих курсов в авторизованных учебных центрах Microsoft.

Достоинства сертификации Microsoft

Программа сертификации Microsoft — один из самых строгих и полных тестов оценки знаний и навыков в области проектирования, разработки и сопровождения программного обеспечения. Сертифицированным специалистом Microsoft становится лишь тот, кто демонстрирует умение решать конкретные задачи, применяя продукты компании. Программа тестирования позволяет не только оценить квалификацию специалиста, но и служит ориентиром для всех, кто стремится достичь современного уровня знаний в этой области. Как и любой другой тест или экзамен, сертификация Microsoft является показателем определенного уровня знаний специалиста, что важно для работодателя и всей организации в целом.

Преимущества сертифицированного специалиста

Звание Microsoft Certified Professional дает Вам:

- официальное признание Ваших знаний и опыта работы с продуктами и технологиями Microsoft;
- доступ к технической информации о продуктах Microsoft через зашишенную область Web-узла MCP;
- эмблемы, демонстрирующие Вашим работодателям и клиентам, что Вы имеете квалификацию сертифицированного специалиста Microsoft;
- приглашения на конференции, семинары и специальные мероприятия Microsoft, предназначенные для специалистов;
- сертификат «Microsoft Certified Professional»;
- подписку на издания Microsoft, содержащие ценную техническую информацию о продуктах и технологиях Microsoft.

Кроме того, в зависимости от типа сертификации и страны сертифицированные специалисты получают:

- годовую подписку на ежемесячно распространяемые компакт-диски Microsoft TechNet Technical Information Network;
- годовую подписку на программу бета-тестирования продуктов Microsoft. В результате Вы бесплатно получите до 12 компакт-дисков с бета-версиями новейших программных продуктов Microsoft.

Выигрыш от сертификации Microsoft для работодателей и организаций

Сертификация позволяет организациям быстро окупить затраты на технологии Microsoft и извлечь максимум прибыли из этих технологий. Исследования показывают, что сертификация сотрудников по программам Microsoft:

- быстро окупается за счет стандартизации требований к обучению специалистов и методов оценки их квалификации;

- позволяет увеличить эффективность обслуживания клиентов, повысить производительность труда и снизить расходы на сопровождение ОС;
- обеспечивает надежные критерии для найма специалистов и их продвижения по службе;
- предоставляет методы оценки эффективности труда персонала;
- обеспечивает гибкие методы переподготовки сотрудников для обучения новым технологиям;
- позволяет оценить партнеров — сторонние фирмы.

Дополнительную информацию о том, какую пользу Ваша компания извлечет из сертификации, см. на странице http://www.microsoft.com/train_cert/cert/bus_bene.htm.

Требования к соискателям

Требования к соискателям определяются специализацией, а также служебными функциями и задачами.

Соискатель сертификата Microsoft должен сдать экзамен, подтверждающий его глубокие знания в области программных продуктов Microsoft. Экзаменационные вопросы, подготовленные с участием ведущих специалистов компьютерной отрасли, отражают реалии применения программных продуктов Microsoft,

- На звание *Сертифицированного специалиста Microsoft* сдают экзамен по работе с одной из операционных систем. Кандидат может сдать дополнительные экзамены, которые подтвердят его право на работу с продуктами Microsoft BackOffice, инструментальными средствами или прикладными программами.
- На звание *Сертифицированного специалиста Microsoft + Интернет* сдают экзамен по Microsoft Windows 2000 Server, поддержке TCP/IP и экзамены по Microsoft Internet Information Server.
- На звание *Сертифицированного специалиста Microsoft + Site Building* сдают два экзамена по основам технологий Microsoft Front Page, Microsoft Site Server и Microsoft Visual InterDev.
- На звание *Сертифицированного системного инженера Microsoft* сдают экзамены по технологии ОС Microsoft Windows, сетевым технологиям и технологиям интегрированного семейства серверных продуктов Microsoft BackOffice.
- На звание *Сертифицированного системного инженера Microsoft + Интернет* сдают 7 экзаменов по операционным системам и два экзамена по выбору.
- На звание *Сертифицированного администратора баз данных Microsoft* сдают три ключевых экзамена и один экзамен по выбору.
- На звание *Сертифицированного разработчика программных решений на основе Microsoft* сдают два экзамена по основам технологии ОС Microsoft Windows и два — по технологиям интегрированного семейства серверных продуктов Microsoft BackOffice.
- На звание *Сертифицированного преподавателя Microsoft* надо подтвердить свою теоретическую и практическую подготовку для ведения соответствующих курсов в авторизованных учебных центрах Microsoft, Более подробные сведения о сертификации по этой программе Вы получите в компании Microsoft по телефону (800) 636-7544 (в США и Канаде) или в ее местном отделении.

Подготовка **к экзаменам**

Существует три режима подготовки: самостоятельная работа, интерактивный режим, а также занятия с инструктором в авторизованных центрах подготовки.

Самостоятельная подготовка

Самостоятельная подготовка — наиболее эффективный метод подготовки для инициативных соискателей. Издательство Microsoft Press предлагает весь спектр учебных пособий для подготовки к экзаменам по программе сертификации специалистов Microsoft. Учебные курсы для самостоятельного изучения, адресованные специалистам компьютерной отрасли, содержат теоретические и практические материалы, мультимедийные презентации, упражнения и необходимое **ПО.** Серия «Mastering» — это интерактивные обучающие компакт-диски для опытных разработчиков. Все эти пособия позволят Вам наилучшим образом подготовиться к сдаче сертификационных экзаменов.

Интерактивная подготовка

Интерактивная подготовка средствами Интернета — альтернатива занятиям в учебных центрах. Вы можете выбрать наиболее удобный распорядок занятий в виртуальном классе, где Вы научитесь работать с продуктами и технологиями Microsoft и подготовитесь к сдаче экзаменов. Интерактивное обучение охватывает множество курсов Microsoft — от обычных официальных до специальных, доступных лишь в интерактивном режиме. Интерактивные ресурсы доступны круглосуточно в авторизованных центрах подготовки.

Авторизованные центры технического обучения

Авторизованные центры технического обучения (Authorized Technical Education Center, ATEC) — самый простой способ пройти курс обучения под руководством опытного инструктора и стать сертифицированным специалистом. Microsoft ATEC — всемирная сеть учебных центров, которые позволяют специалистам повысить свой технический потенциал под руководством сертифицированных инструкторов Microsoft.

Список центров ATEC в США и Канаде можно получить в факсимильной службе Microsoft — тел. (800) 727-3351. За пределами США и Канады обращайтесь в местные отделения Microsoft.

Техническая поддержка

Мы постарались сделать все от нас зависящее, чтобы и учебный курс, и прилагаемый к нему компакт-диск не содержали ошибок. Издательство Microsoft Press публикует постоянно обновляемый список исправлений и дополнений к своим книгам по адресу http://mspress.microsoft.com/support/.

Если все же у Вас возникнут вопросы или Вы захотите поделиться своими предложениями или комментариями, обращайтесь в издательство Microsoft Press по одному из указанных ниже адресов:

Электронная почтя: TKINPUT@MICROSOFT.COM

Почтовый адрес: Microsoft Press
Attn:MCSE Training Kit-Microsoft Windows 2000 Server Editor
One Microsoft Way
Redmond,WA 98052-6399

ГЛАВА 1

Знакомство с Microsoft Windows 2000

В этой главе

Данная глава содержит обзор семейства продуктов Microsoft Windows 2000 и архитектуры системы. Также здесь обсуждаются концепции единой службы каталогов Windows 2000 Server, Advanced Server и Datacenter Server — Active Directory.

Прежде всего

Для изучения материалов этой главы не нужно специальных знаний, хотя опыт работы с Microsoft Windows NT может оказаться полезным.

Занятие 1. Обзор Windows 2000

Это занятие познакомит Вас с семейством продуктов Windows 2000: Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server и Windows 2000 Datacenter Server. Вы узнаете о характеристиках и преимуществах Windows 2000 в основном на примере Windows 2000 Professional и Windows 2000 Server.

Изучив материал этого занятия, Вы сможете:

- ✓ описать основные возможности четырех ОС семейства Windows 2000 и различия между ними.

Продолжительность занятия — около 15 минут.

Семейство Windows 2000

Windows 2000 — многоцелевая ОС со встроенной поддержкой одноранговых и клиент-серверных сетей. Семейство продуктов Windows 2000 было разработано для повышения надежности, доступности и масштабируемости. Windows 2000 включает технологии, снижающие совокупную стоимость владения (ССВ) за счет удешевления обслуживания вычислительной техники. Кроме того, Windows 2000 — великолепная среда для построения серверов приложений и Интернета.

Все продукты семейства Windows 2000: Professional, Server, Advanced Server и Datacenter Server — поддерживают экономически эффективную, легко адаптируемую инфраструктуру клиент-сервер на платформе IBM PC. Платформа Windows 2000 предоставляет администраторам широкие возможности по управлению сетью и инфраструктурой клиент-сервер, максимально гибко реализуя централизованный контроль, обычно ассоциируемый с моделью мэйнфрейм-терминал.

Windows 2000 Professional

Это основная ОС для настольных компьютеров, применяемых в бизнесе. Эта высокопроизводительная, защищенная клиентская ОС объединяет в себе лучшие качества Windows 98 и традиционную мощь Windows NT Workstation. Новая ОС имеет несколько упрощенный пользовательский интерфейс, включает поддержку Plug-n-Play и расширенное управление электропитанием, различных аппаратных средств. В сравнении с Windows NT Workstation в Windows 2000 Professional значительно увеличена управляемость, надежность и безопасность за счет новой файловой системы с возможностью шифрования и средств управления приложениями.

Windows 2000 Server

Эта серверная платформа способна функционировать как сервер файлов, печати, приложений или Web-сервер. Данная ОС включает все возможности Windows 2000 Professional и массу новых функций. В основе Windows 2000 лежит набор служб инфраструктуры, основанный на Active Directory, централизующей управление сетевыми ресурсами, пользователями, группами и службами безопасности. Windows 2000 Server поддерживает системы, включающие до четырех процессоров и ОЗУ объемом до 4 Гб. Также она включает функции для эффективного обслуживания рабочих групп и филиалов организаций и совместного использования серверов файлов, печати, Web-серверов и коммуникационных серверов. Windows 2000 Server идеально подходит для малого и среднего бизнеса.

Windows 2000 Advanced Server

Эта ОС. выполняющая функции сервера приложений, включает в себя возможности Windows 2000 Server и имеет отличные характеристики доступности и масштабируемости, что очень важно для сетей крупных предприятий. Windows 2000 Advanced Server поддерживает до 8 процессоров и двустороннюю кластеризацию, отличающуюся высокой степенью доступности. Это идеальная ОС для интенсивной работы с крупными базами данных. Аппаратные средства, разработанные с учетом технологии Intel Physical Address Extensions (PAEs), позволяют ей адресовать большие объемы физической памяти.

Windows 2000 Datacenter Server

Это специализированная версия Windows 2000 Server, разработанная для крупных предприятий и оптимизированная для работы с большими хранилищами данных, эконометрического анализа, научного моделирования, оперативной обработки транзакций и масштабных серверных проектов. Это лучшее решение для поставщиков услуг Интернета и размещения Web-узлов. Windows 2000 Datacenter Server включает возможности Windows 2000 Advanced Server, службы балансировки нагрузки и 4-узловой кластеризации. Поддерживает от 16 до 32 процессоров за счет расширений ОС, изготовленных *производителями аппаратуры* (Original Equipment Manufacturer, OEM).

Характеристики Windows 2000

В таблице описаны возможности Windows 2000 Professional и Windows 2000 Server.

Характеристика	Преимущество
Низкая совокупная стоимость владения	Стоимость эксплуатации и администрирования сети снижена за счет автоматической установки и обновления приложений, а также упрощения настройки компьютеров клиентов. Необходимость обращаться в службу поддержки возникает реже, так как применен хорошо знакомый пользователям и администраторам интерфейс Microsoft Windows, мастера и справочная система. Администратор не «бегает» к компьютерам пользователей для обновления ОС.
Безопасность	Безопасность обеспечивается на локальном и сетевом уровнях. Реквизиты пользователя проверяются до того, как он получит доступ к ресурсам и данным компьютера или сети, также выполняется аудит файлов, папок, принтеров и других ресурсов. Поддерживается протокол Kerberos и инфраструктура открытого ключа.
Служба каталогов	Содержит информацию о ресурсах сети: учетных записях пользователей, приложениях, ресурсах печати и параметрах безопасности.
	Отвечает за предоставление пользователям доступа к ресурсам по всей сети Windows 2000. Позволяет определить местоположение пользователей, компьютеров и ресурсов в сети и управлять ресурсами и их безопасностью.
	Windows 2000 Server содержит всю информацию служб Active Directory в каталоге, который и является базой данных, хранящей сведения о сетевых ресурсах: компьютерах и принтерах. Службы Active Directory обеспечивают доступ пользователям и приложениям к этой информации, что также облегчает управление доступом к ресурсам.

(*окончание*)

Характеристика	Преимущество
Производительность и масштабируемость	Поддерживает архитектуру *симметричной многопроцессорной обработки* (Symmetric Multiprocessing, SMP) на компьютерах с несколькими процессорами, обеспечивает поддержку многозадачности.
	Windows 2000 Server поддерживает до четырех процессоров. Компьютеры с этой ОС обычно настраиваются как серверы файлов, печати или приложений, например, как серверы терминалов.
	Windows 2000 Professional поддерживает до двух процессоров.
Работа в сети и коммуникационные службы	Включает встроенную поддержку наиболее известных протоколов: TCP/IP и IPX/SPX. Обеспечивает взаимодействие с сетями Novell NetWare, UNIX и AppleTalk. Обеспечивает удаленным доступ к сетям, что позволяет мобильным пользователям подключаться к Windows 2000-компьютерам.
	Windows 2000 Server поддерживает одновременно до 256 входящих сеансов удаленного доступа.
	Windows 2000 Professional поддерживает один входящий сеанс удаленного доступа.
Интеграция с Интернетом	Пользователи могут безопасно просматривать ресурсы рабочей или корпоративной сети и Интернета, работать с электронной почтой.
	Windows 2000 Server включает Microsoft Internet Information Services (IIS) — платформу Web-сервера для размещения Web-узлов в Интернете и интрасетях.
	Windows 2000 Professional включает персональный Web-сервер, допускающий небольшое число подключений.
Встроенные средства администрирования	Вы можете создавать нестандартные средства управления локальными и удаленными компьютерами с единым интерфейсом и объединять в стандартном интерфейсе средства администрирования сторонних фирм.
Поддержка аппаратуры	Поддерживает технологию *универсальной последовательной шины* (Universal Serial Bus, USB), устраняющей многие ограничения старых периферийных устройств. PnP-устройства обнаруживаются, устанавливаются и настраиваются автоматически.

Резюме

Семейство продуктов Windows 2000 включает Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server и Windows 2000 Datacenter Server. Windows 2000 Professional — это настольная ОС со встроенной поддержкой одноранговых и клиент-серверных сетей. Windows 2000 Server включает возможности Windows 2000 Professional и массу новых серверных функций. Windows 2000 Server можно использовать как сервер файлов, печати, приложений или Web-сервер. Windows 2000 Advanced Server — более мощная ОС сервера приложений, основанная на Windows 2000 Server и дополненная двусторонней кластеризацией, поддержкой большего числа процессоров и одновременных подключений пользователей. Это самая мощная система для крупных предприятий, предлагаемая Microsoft.

Занятие 2. Архитектура операционной системы

Windows 2000 — это модульная система, состоящая из небольших независимых программных компонентов, совместно выполняющих разные задачи. Каждый компонент предоставляет определенные функции, которые служат своеобразным интерфейсом для остальной части системы.

Изучив материал этого занятия, Вы сможете:

- ✓ определить основные компоненты архитектуры Windows 2000;
- ✓ различать компоненты режима ядра и пользовательского режима;
- ✓ определить характеристики драйверов режима ядра, включая WDM-драйверы.

Продолжительность занятия — около 45 минут.

Обзор архитектуры Windows 2000

Поскольку Windows 2000 спроектирована для работы на компьютерах и с CISC-, и с RISC-процессорами, устройства и их драйверы можно конфигурировать как аппаратно, так и программно. Windows 2000 поддерживает вытесняющую многозадачность и способна работать, одинаково эффективно используя как одно-, так и многопроцессорные системы. При этом гарантируется, что код, выполняемый на одном процессоре, не получит доступ и не модифицирует данные, обрабатываемые другим процессором. Windows 2000 поддерживает пакетный ввод-вывод с применением возвратных *пакетов запросов ввода-вывода* (I/O request packets, IRP) и асинхронный ввод-вывод. Благодаря этому процесс — отправитель запроса ввода-вывода продолжает выполняться, не ожидая ответа на отправленный запрос. Windows 2000 разработана как модульная система, которая состоит из объектов, работающих либо в *пользовательском* (user) режиме, либо режиме *ядра* (kernel).

Как и все ОС, Windows 2000 имеет программный код, отвечающий за доступность аппаратных средств в приложениях. На рис. 1-1 изображена концептуальная структура, иллюстрирующая взаимодействие элементов системы.

Режим пользователя

Уровень режима пользователя (user mode layer) Windows 2000 состоит из наборов компонентов, называемых *подсистемами* (subsystem), — внутренних и внешних. Подсистема передает запросы ввода-вывода драйверам режима ядра через службы ввода-вывода. Она устроена так, что приложения и конечные пользователи ничего не знают о компонентах режима ядра.

Внешние подсистемы

Внешние подсистемы (environment subsystems) позволяют Windows 2000 выполнять и запускать приложения, разработанные для разных ОС. Они эмулируют разные ОС, используя *интерфейсы прикладного программирования* (application programming interface, API). Внешние подсистемы перехватывают API-вызовы приложения, переводят их в формат, понятный Windows 2000, и передают исполняемым компонентам режима ядра.

Таблица содержит описания внешних подсистем Windows 2000.

Внешняя подсистема	Назначение
Win32	Управляет приложениями Win32 и обеспечивает среду для работы приложений Win16 и MS-DOS.
POSIX	Предоставляет API-интерфейсы POSIX-приложениям. POSIX — стандарт IEEE — гарантирует переносимость приложений на разные платформы.

Внешние подсистемы и приложения, запущенные в пределах этих подсистем, не имеют прямого доступа к аппаратным устройствам или драйверам. Они ограничены выделенным им адресным пространством. Внешние подсистемы вынуждены использовать дисковое пространство в качестве виртуальной памяти каждый раз, когда системе требуется память. Кроме того, они выполняются с более низким приоритетом, чем процессы режима ядра, а значит, реже получают доступ к процессору.

Примечание Архитектура Microsoft Enterprise Memory Architecture (EMA) является частью Windows 2000 Advanced Server и Windows 2000 Datacenter Server и предоставляет больше ОЗУ для приложений, повышая их производительность.

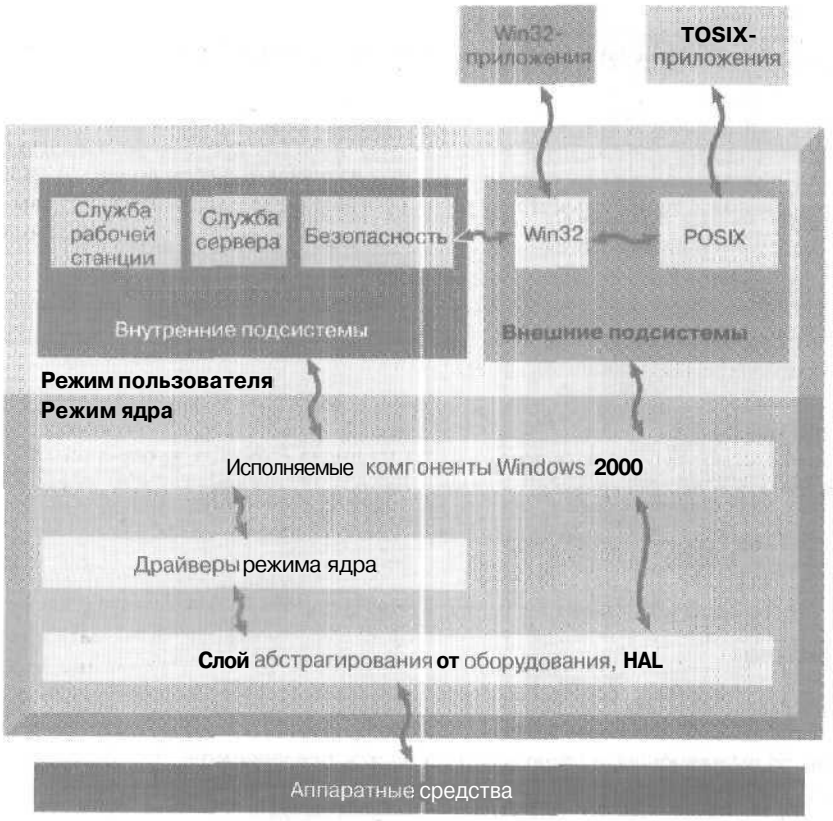


Рис. 1-1. Взаимодействие элементов Windows 2000

Внутренние подсистемы

Внутренние подсистемы (integral subsystems) выполняют основные функции ОС. Вот некоторые из них:

Внутренняя подсистема	Функция
Подсистема безопасности	Создает маркеры доступа и отслеживает права и разрешения, связанные с учетными записями пользователей. Принимает запросы регистрации пользователей и инициирует проверку подлинности входа в систему. Отвечает за аудит системных ресурсов.
Служба рабочей станции	Внутренняя сетевая подсистема, предоставляющая API-интерфейс для доступа к сетевому перенаправителю (redirector). Позволяет компьютеру работать в сети.
Служба сервера	Внутренняя сетевая подсистема, предоставляющая API-интерфейс для доступа к сетевому серверу. Обслуживает доступ к ресурсам из сети.

Режим ядра

Уровень режима ядра (kernel mode layer) имеет доступ к системным данным и аппаратным средствам. Компоненты в режиме ядра могут напрямую обращаться к памяти и выполняются в зашишенном адресном пространстве, Последовательность выполнения кода обусловлена *приоритетами* (prioritizing criteria) — атрибутами, которыми обладает каждый выполняемый *поток* (thread). В режиме ядра приоритеты назначаются всем аппаратным и программным прерываниям, причем некоторая часть программного кода режима ядра выполняется на высшем *уровне прерываний* (interrupt request level, IRQL). Уровень режима ядра включает несколько типов компонентов, выполняющих строго определенные функции: Executive (исполняемые компоненты Windows), *слой абстрагирования от оборудования* (Hardware Abstraction Layer, HAL) и набор драйверов режима ядра.

Исполняемые компоненты Windows 2000

Выполняют основную работу по управлению объектами и вводом-выводом, включая управление безопасностью. Внутренние компоненты из числа Executive вроде диспетчеров виртуальной памяти и ввода-вывода определяют один или несколько типов объектов. Все эти компоненты обеспечивают работу системных служб и выполнение подпрограмм. Системные службы доступны как подсистемам пользовательского режима, так и прочим исполняемым компонентам. Внутренние подпрограммы доступны только компонентам из числа Executive. Ни один компонент не имеет прямого доступа к экземпляру объекта другого типа. Для использования объекта другого компонента необходимо вызвать внешнюю подпрограмму. Каждый компонент экспортирует подпрограммы, поддерживающие взаимодействие с ядром системы. При вызове они манипулируют экземплярами объектов определенных типов. Если реализация поддерживающей подпрограммы с течением времени изменяется, то вызывающая подпрограмма остается переносимой, поскольку внешний интерфейс не меняется.

В таблице перечислены компоненты режима ядра из числа Executive.

Компонент	Описание
Диспетчер ввода-вывода (I/O Manager)	Предоставляет службы ядра драйверам устройств и преобразует команды чтения-записи пользовательского режима в формат IRP Управляет вводом-выводом устройств и включает компоненты:
	файловые системы принимают запросы ввода-вывода и переводят их в аппаратно-зависимые вызовы; сетевой перенаправитель и сетевой сервер реализованы как драйверы файловых систем;
	драйверы устройств — это драйверы низкого уровня, которые для приема сигналов ввода-вывода работают с аппаратурой напрямую;
	диспетчер кэша ускоряет ввод-вывод (сохраняя в системной памяти результаты обращения к диску) и запись (кэшируя их в фоновом режиме).
Эталонный монитор безопасности	Следит за соблюдением политики безопасности на локальном компьютере.
Диспетчер межпроцессного взаимодействия (Interprocess Communication, Manager IPC)	Управляет взаимодействием клиента и сервера, внешними подсистемами и исполняемой системой. Подсистемы действуют подобно клиенту, запрашивающему информацию, а исполняемая система — подобно серверу, удовлетворяющему этот запрос. Включает два типа компонентов:
	средства локального вызова процедур (Local Procedure Call, LPC) управляют взаимодействием клиента и сервера, расположенных на одном компьютере;
	средства удаленного вызова процедур (Remote Procedure Call, RPC) управляют взаимодействием клиента и сервера, расположенных на разных компьютерах.
Диспетчер виртуальной памяти (Virtual Memory Manager, VMM)	Управляет виртуальной памятью — собственным адресным пространством каждого процесса. VMM позволяет ОС использовать память на жестком диске как часть физической памяти. VMM также контролирует подкачку — процесс перемещения программного кода и данных из физической памяти на диск и обратно.
Диспетчер процессов	Создает и завершает процессы (программы или часть программ) и потоки (особые наборы команд внутри программ). Приостанавливает и возобновляет выполнение потоков, сохраняет и извлекает информацию о процессах и потоках.
Диспетчер PnP	Централизованно управляет процессом PnP. Обеспечивает распознавание PnP-устройств с момента загрузки, служит средством связи с HAL, с исполнительной системой и драйверами устройств. Заставляет драйверы шины выполнять нумерацию, конфигурирование, добавление и запуск устройств. Взаимодействует с PnP-частью пользовательского режима для временной остановки или удаления устройств,

(окончание)

Компонент	Описание
Диспетчер электропитания	Управляет API-интерфейсами питания, координирует события питания и генерирует IRP-пакеты питания. Например, если несколько устройств посылают запрос на выключение, диспетчер определяет те, что должны быть сериализованы, и генерирует соответствующий IRP-пакет.
Оконный диспетчер и интерфейс графических устройств (Graphic Device Interface. GDI)	Управляют системой отображения. Эти компоненты. реализованные в одном драйвере Win32k.sys, выполняют следующие функции: оконный диспетчер управляет отображением окон и выводом на экран, отвечает за прием ввода от клавиатуры и мыши и передает его приложениям. GDI включает функции, требующиеся для прорисовки и управления графикой.
Диспетчер объектов	Создает, удаляет и управляет объектами, представляющими ресурсы системы: процессами, потоками и структурами данных.

Уровень HAL

Уровень абстрагирования от оборудования (Hardware Abstraction Layer, HAL) скрывает, или «виртуализирует», детали аппаратного интерфейса, что позволяет переносить Windows 2000 на другие платформы. Содержит код, ориентированный на работу с оборудованием, который оперирует интерфейсом ввода-вывода, контроллером прерываний и механизмом многопроцессорного взаимодействия. Первоначально был разработан, чтобы Windows 2000 могла работать как на оборудовании с элементной базой Intel, так и на любой другой платформе, например, на системах с процессорами Alpha.

Примечание Поддержка платформы Alpha прекращена после выпуска Windows 2000 Release Candidate One. См. также документ *\chapt01\articles\compaq.html* на прилагаемом компакт-диске.

HAL, реализованный как *динамически подключаемая библиотека* (DLL), отвечает за взаимодействие компонентов системы с конкретным оборудованием. HAL экспортирует подпрограммы поддержки, скрывающие подробности реализации специфических элементов аппаратуры: кэшей, шин ввода-вывода и контроллеров прерываний. HAL также обеспечивает интерфейс между аппаратурой платформы и программными компонентами системы.

Драйверы режима ядра

Как и сама ОС, драйверы режима ядра реализованы как отдельные модульные компоненты со строго определенными функциональными возможностями. Все драйверы режима ядра, включая драйверы *модели драйверов Windows* (Windows Driver Model, WDM), содержат стандартные системные подпрограммы и некоторые внутренние подпрограммы в зависимости от индивидуальных требований устройств. Для прочих компонентов системы, включая программный код пользовательского режима, соединение с устройством представляется как операция открытия файла через *диспетчер ввода-вывода* (I/O Manager). Впрочем, внутри системы ввода-вывода логические, виртуальные и физические устрой-

ства для каждого драйвера представляются в виде объектов устройств. Загрузочный образ каждого драйвера представляется внутри диспетчера ввода-вывода как объект драйвера. Диспетчер определяет типы объектов для объектов файлов, устройств и драйверов. Драйверы обращаются к ним через подпрограммы режима ядра, экспортируемые диспетчером ввода-вывода и другими компонентами системы.

При проектировании драйверов режима ядра преследовались те же цели, что и при разработке Windows 2000:

- переносимость с одной платформы на другую;
- обеспечение работоспособности при изменении конфигурации программных и аппаратных средств;
- поддержка вытесняющей многозадачности;
- надежная работа в многопроцессорных системах;
- объектно-ориентированная архитектура;
- поддержка пакетного ввода-вывода с возвратными IRP-пакетами;
- поддержка асинхронного ввода-вывода.

Существует три основных типа драйверов режима ядра: высшего, среднего и низшего уровней (рис. 1-2).

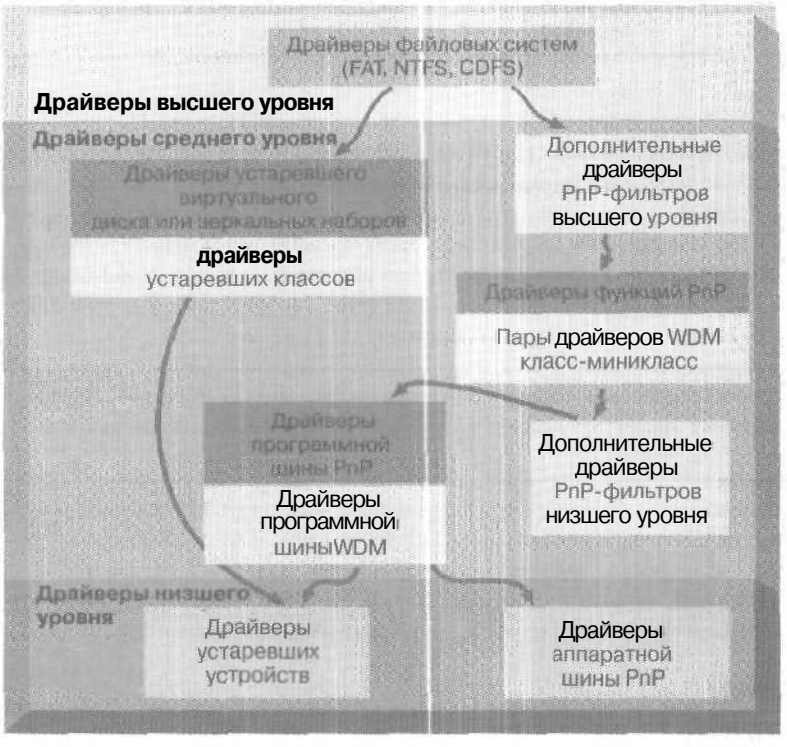


Рис. 1-2. Типы драйверов режима ядра

Эти типы, сходные по структуре, совершенно разнятся по возможностям, что видно из следующей таблицы (заметьте: WDM-драйверы относятся к среднему уровню).

Тип драйвера	Описание
Драйверы высшего уровня	Включают *драйверы файловых систем* (file system driver, FSD): *таблицу размещения файлов* (file allocation table, FAT), *файловую систему Windows NT* (NT file system, NTFS), *файловую систему компакт-дисков* (compact disk file system, CDFS). Зависят от поддержки драйверов нижних уровней. Каждый FSD зависит от поддержки от одного или более нижележащих драйверов периферийных устройств.
Драйверы среднего уровня	Включает драйвер виртуального диска, зеркального набора, а также драйверы класса, зависящие от типа устройства. Зависят от поддержки драйверов низшего уровня. Включают также: драйверы **PnP-функций**, управляющие определенными периферийными устройствами путем ввода-вывода, контролируемого драйвером аппаратной шины PnP; драйверы **PnP-фильтров**, размещаемые в стеке драйверов периферийных устройств до или после драйверов PnP-функций; любые системные драйверы классов, которые экспортируют системный интерфейс WDM-класс/минипорт; драйверы программной шины PnP, представляющие набор дочерних устройств, к которым могут присоединяться высокоуровневые драйверы класса, функции или фильтры; **драйверы программной шины WDM**.
Драйверы низшего уровня	Это может быть, например, драйвер аппаратной шины PnP, контролирующий шину *ввода-вывода*, к которой подключены периферийные устройства. Драйверы этого типа не зависят от нижележащих драйверов, однако управляют периферийными физическими устройствами. Также включают устаревшие драйверы, управляющие периферийными физическими устройствами напрямую, например, драйвер хост-адаптера шины SCSI.

Модель драйверов Windows

Некоторые из драйверов режима ядра Windows 2000 также являются WDM-драйверами, относящимися к подмножеству драйверов среднего уровня. Спецификация WDM определяет архитектуру и интерфейс взаимодействия с ОС драйверов аппаратуры. Устройства, соответствующие WDM, выигрывают от использования общего набора служб ввода-вывода WDM и совместимы на уровне двоичного кода с Windows 98 и Windows 2000.

WDM упрощает разработку драйверов аппаратуры для поддержки всех платформ Windows и позволяет устанавливать и использовать устройства на компьютерах с Windows 98 и 2000. WDM-драйверы построены на основе структуры класс-минипорт, обеспечивающей модульную, наращиваемую архитектуру для поддержки устройств. WDM является базовой технологией для Simply Interactive PC (SIPC), инициативы Zero Administration, поддержки новых PnP-устройств для шин USB и IEEE 1394, а также для новой технологии управления питанием OnNow.

Каждый класс WDM абстрагирует большинство общих деталей, вовлеченных в процесс управления схожими устройствами. Например, представьте пять устройств, подключенных к шине USB. Если каждый из их драйверов содержал бы весь код, необходимый

для взаимодействия со своим устройством, получилось бы пять очень больших драйверов, в основном состоящих из одного и того же кода для взаимодействия с USB. Для разработки WDM-драйвера надо написать более мелкие части программного кода (минипорты), которые взаимодействуют напрямую с оборудованием и обращаются к драйверу соответствующего класса для выполнения общих задач. Кроме того, при написании минипорта снижается вероятность появления ошибок в программном коде драйвера устройства.

Многоуровневая архитектура WDM

WDM — это многоуровневая архитектура, использующая специальные драйверы классов для обеспечения переносимости. Классы драйверов являются уровнями абстракции, что позволяет использовать WDM-драйверы как в Windows 2000, так и в Windows 98. Существует четыре класса драйверов:

- драйверы минипортов;
- драйверы классов;
- службы ОС;
- виртуальные драйверы.

Каждому классу шины и классу аппаратуры, поддерживаемому моделью WDM, в Windows 2000 соответствует драйвер класса. Microsoft обеспечивает специфическую для платформы поддержку WDM, поэтому для всех аппаратных устройств, классы которых поддерживаются Microsoft, требуется написать только драйверы минипортов.

Драйверы минипортов уже реализованы в Windows 2000 в классах SCSI-устройств и сетевых адаптеров. В Windows 2000 концепция драйвера минипорта расширена для поддержки шины USB. Драйверы минипорта:

- косвенно контролируют оборудование через соответствующий драйвер класса шины;
- совместимы на уровне двоичного кода для всех платформ Windows;
- динамически загружаются и выгружаются;
- реализуют функциональные возможности конкретного устройства класса;
- поддерживают несколько интерфейсов классов.

Драйверы классов — по сути «драйверы для драйверов». Предоставляют интерфейсы между разными уровнями архитектуры WDM. Нижний уровень драйвера класса взаимодействует с интерфейсом конкретного класса, представленным драйвером минипорта. Верхняя граница драйверов класса высшего уровня зависит от конкретной ОС. Драйверы классов:

- реализуют функции класса устройств, не относящиеся к работе конкретных устройств или шин, кроме драйверов классов шин;
- динамически загружаются и выгружаются;
- реализуют функции, специфичные для класса (нумерацию);
- предоставляют единый интерфейс конкретного класса для множества уровней клиентов.

Службы операционной системы. Их уровень индивидуален для ОС. Этот уровень абстрагирует функциональность ОС от нижележащего уровня драйверов минипортов, а именно:

- управляет потоками;
- управляет «кучей» (heap);
- обрабатывает **события.**

Виртуальные драйверы, реализованные еще в Microsoft Windows 3.0, — это знакомьте Вам по Windows 95 VXD-файлы и файлы с расширением .386 в старых версиях Windows. В WDM выполняют несколько специализированных функций, абстрагируют интерфейсы унаследованного оборудования и посылают реализованные в классе команды соответствующим устройствам. Например, игра для MS-DOS, запущенная под Windows, будет использовать виртуальный драйвер для работы с джойстиком, подключенным к шине USB.

Эти драйверы, не имея прямого доступа к аппаратуре, действуют как посредники, чтобы старые программные или аппаратные средства корректно работали в незнакомой архитектуре.

Поддержка WDM-драйверов в Windows 2000 включает;

- драйвер класса потоков для поддержки в режиме ядра потоков данных, генерируемых в ходе оцифровки видео, работы MPEG-декодеров, программ записи и воспроизведения звука, DVD-дисков и широковещания;
- драйвер класса HID для поддержки устройств ввода;
- драйвер класса шины USB;
- драйвер класса шины IEEE 1394.

Резюме

Модульная ОС Windows 2000 состоит из небольших самостоятельных программных компонентов, совместно выполняющих разные задачи. Объекты Windows 2000 работают либо в режиме ядра, либо в режиме пользователя. Основные компоненты уровня пользовательского режима — группа подсистем, изолирующих конечных пользователей и приложения от необходимости знать что-либо о компонентах режима ядра. Существует два типа подсистем: внешние и внутренние. Основными компонентами уровня режима ядра являются Executive (исполняемые компоненты Windows), уровень HAL и драйверы режима ядра. Executive выполняет основную работу по управлению вводом-выводом и объектами, включая безопасность. HAL скрывает подробности аппаратных интерфейсов и заведует интерфейсами ввода-вывода, контроллерами прерываний, механизмами межпроцессного взаимодействия. Драйверы режима ядра реализованы как дискретные, модульные компоненты со строго определенным набором функциональных возможностей. Существует три типа драйверов режима ядра: высшего, среднего и низшего уровней. WDM-драйверы являются подмножеством драйверов среднего уровня режима ядра.

Занятие 3, Служба каталогов Windows 2000

Каталог (directory) — это хранимый набор сведений о взаимосвязанных объектах. Сетевой каталог можно сравнить с телефонным справочником, содержащим имена, адреса и телефоны людей и предприятий — набор атрибутов (имен и адресов), используемых для поиска сведений об объектах каталога (телефонных номерах). Точно так же *служба каталогов* (directory service) однозначно идентифицирует и организует пользователей и ресурсы сети и обеспечивает к ним доступ.

Изучив материал этого занятия, Вы сможете:

- ✓ описать функции службы каталогов;
- ✓ пояснить различия между рабочими группами и доменами;
- ✓ описать службу каталогов Active Directory и перечислить ее структурные компоненты.

Продолжительность занятия - - около 45 минут.

Знакомство со службой каталогов

В распределенной компьютерной системе или глобальной компьютерной сети, скажем, в Интернете, существует множество объектов: пользователи, файловые серверы, принтеры, факс-серверы, приложения и базы данных. Пользователи хотят получать к ним легкий и быстрый доступ, а администраторы — управлять работой с ними. Если необходимая для этого информация хранится централизованно, процесс поиска и управления этими объектами значительно упрощается. В этом помогает служба каталогов.

Терминами *каталог* и *служба каталогов* обозначают каталоги в общедоступных и частных сетях. Каталог содержит сведения о ресурсах сети. Служба каталога является одновременно *источником* (source) информации о каталоге и *службой* (service), обеспечивающей доступ к ней пользователей.

Служба каталогов предоставляет средства для организации и облегчения доступа к ресурсам сетевых компьютерных систем Она позволяет искать объекты по одному или нескольким атрибутам. Например, администраторы могут знать не точное имя объекта, а лишь один или несколько его атрибутов. Службы каталогов позволяют им запросить список объектов, отвечающих известным атрибутам, например, перечень цветных принтеров на третьем этаже.

Служба каталогов применяется для:

- защиты объектов в БД каталога отвторжений извне или неуполномоченных пользователей интрасети;
- репликации каталога на другие компьютеры в сети, для обеспечения доступа к нему других пользователей и отказоустойчивости;
- дробления каталога на несколько хранилищ, расположенных на разных компьютерах сети; это позволяет хранить крупные каталоги, содержащие много объектов.

Служба каталога — это инструмент и администратора, и пользователя. По мере расширения сети требуется управлять все большим количеством ресурсов, и здесь служба каталогов незаменима.

Рабочие группы и домены

Служба каталогов упорядочивает сетевые ресурсы и упрощает к ним доступ. Для облегчения доступа Windows 2000 поддерживает два типа сетей: рабочие группы и домены.

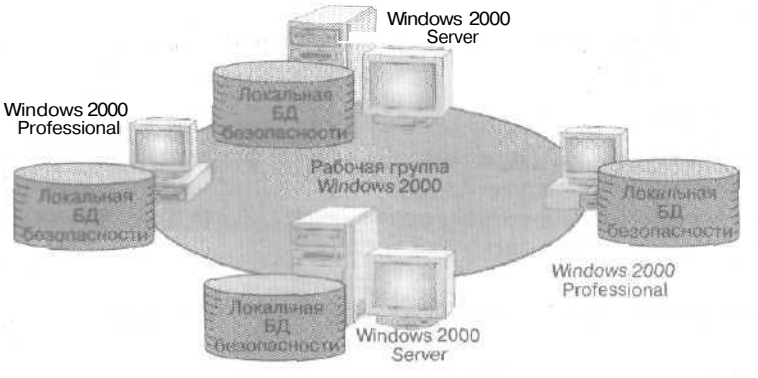
Рабочая группа Windows 2000

Рабочая группа (workgroup) — это логическая группировка объединенных в сеть компьютеров, предоставляющих доступ к ресурсам, скажем, к файлам и принтерам. *Домен* (Domain) — это логическая группировка объединенных в сеть компьютеров, предоставляющих доступ к централизованной БД каталога, содержащего учетные записи пользователей и информацию о безопасности для данного домена. Рабочую группу иногда сравнивают с одноранговой сетью, так как все компьютеры в ней могут совместно обращаться к ресурсам без выделенного сервера (рис. 1-3). Каждый компьютер с Windows 2000 Server и Windows 2000 Professional, входящий в рабочую группу, ведет свою БД безопасности, содержащую учетные записи пользователей и информацию безопасности для данного компьютера.

Поскольку каждый компьютер в рабочей группе ведет свою БД безопасности, администрирование учетных записей пользователей и доступа к ресурсам децентрализовано. Пользователь должен иметь учетную запись на каждом компьютере, к которому ему нужен доступ. Любые изменения учетных записей пользователя, например, смену пароля или добавление новой учетной записи, нужно проделывать на каждом компьютере. Если Вы забыли добавить новую учетную запись на одном из компьютеров, пользователь не получит доступа к его ресурсам.

Рабочие группы Windows 2000 обеспечивают следующие преимущества:

- для централизованного хранения БД безопасности не требуется компьютер с Windows 2000 Server;
- их простосоздать, они не требуют такого детального планирования и администрирования, как домен;



Рис, 1-3. Рабочая группа Windows 2000

- удобны для небольшого количества расположенных рядом компьютеров; в сетях, объединяющих более 10 компьютеров, рабочие группы неэффективны;
- удобны для небольших групп опытных пользователей, способных грамотно распределять ресурсы.

Примечание В рабочей группе компьютер с Windows 2000 Server называется *изолированным сервером* (stand-alone server).

Домен Windows 2000

Это логическая группировка сетевых компьютеров с общей БД каталога, содержащей учетные записи пользователей и правила безопасности домена. В Windows 2000 эта БД называется каталогом и по сути является частью Active Directory — службы каталогов Windows 2000. В домене каталог хранится на контроллерах домена (рис. 1-4). *Контроллер домена* (domain controller) — это сервер, управляющий всеми действиями пользователей, связанными с безопасностью в домене, и обеспечивающий централизацию администрирования.

Примечание В доменах Windows NT существовала иерархия контроллеров домена: *резервные* (backup domain controller, BDC) и *главные* (primary domain controllers, PDCs). В Windows 2000 все контроллеры домена равноправны.

Рис. 1-4. Домен Windows 2000

Домен не относится к конкретному расположению или конфигурации сети. Компьютеры в домене могут находиться близко друг к другу в малой ЛВС или в разных уголках мира, соединяясь по линиям связи, включая аналоговые, ISDN или DSL. Подробнее о доменах см. следующий раздел этой главы.

Домены Windows 2000:

- предоставляют централизованное администрирование, поскольку информация о пользователях хранится централизованно;
- обеспечивают однократный вход в систему пользователей с получением доступа к разрешенным ресурсам, например к файлам, сетевым принтерам и приложениям; пользователь, войдя в систему на одном компьютере, может работать с ресурсами на другом с учетом срока действия разрешения для данного ресурса;
- обеспечивают масштабирование, позволяя создавать очень большие сети.

Служба каталогов Active Directory

Включена в Windows 2000 и обеспечивает централизованное управление сетью, позволяя легко добавлять, удалять и перемещать ресурсы, например учетные записи пользователей, принтеры, серверы, БД, группы, компьютеры, политики безопасности, которые хранятся в каталоге в виде объектов.

Особенности Active Directory

Active Directory иерархически организует ресурсы в домене — основной единице репликации и безопасности в сети Windows 2000. Каждый домен включает один или несколько контроллеров, на которых хранится полная реплика (копия) каталога домена. Для упрощения администрирования все контроллеры домена в Active Directory равноправны, поэтому изменения, выполненные на любом контроллере домена, можно реплицировать на остальные.

Масштабируемость

В Active Directory каталоги хранят информацию, используя *разделы* (partitions), которые логически делят каталог и обеспечивают хранение большого количества объектов. Это позволяет увеличивать его по мере роста предприятия — от нескольких сотен до миллионов объектов.

Поддержка открытых стандартов

Active Directory объединяет в себе концепцию пространства имен Интернета со службой каталогов Windows NT. Это позволяет объединять и управлять различными пространствами имен в разнородных аппаратных и программных средах. Active Directory применяет *доменную систему имен* (Domain Name System, DNS) и может обмениваться данными с любым приложением или каталогом, использующим протокол LDAP. Active Directory предоставляет доступ к своей информации из других служб каталогов, поддерживающих LDAP версий 2 и 3, например из службы каталогов Novell NetWare — Novell Directory Services, NDS.

Доменная система имен

Поскольку Active Directory использует DNS как службу доменных имен и поиска, ичена доменов Windows 2000 являются также именами DNS. Windows 2000 Server использует динамическую DNS, позволяющую клиентским компьютерам с динамическими адресами регистрироваться прямо на сервере DNS и динамически обновлять таблицу DNS. Динамическая DNS устраняет необходимость в других службах именования Интернета, например WINS.

Примечание Для корректной работы Active Directory и связанного ПО надо установить и настроить службу DNS.

Упрощенный протокол доступа к каталогам

Active Directory отвечает стандартам Интернета и поддерживает LDAP. LDAP — стандарт Интернет (RFC 1777) для доступа к службе каталогов — был разработан как упрощенная альтернатива *протоколу доступа к каталогам* (Directory Access Protocol, DAP) X.500. X500 — набор стандартов, созданный ISO и определяющий распределенную службу каталогов. Active Directory поддерживает LDAP версий 2 и 3 и использует его для обмена данными между каталогами и приложениями.

Примечание См. документ \chapt01\articles\RFC 1777.txt на прилагаемом к книге компакт-диске.

Поддержка стандартных форматов имен

Active Directory поддерживает несколько общих форматов имен, что позволяет приложениям и пользователям получать доступ к каталогу, применяя наиболее удобный для них формат. Вот несколько стандартных форматов имен, поддерживаемых Active Directory:

Формат	Описание
RFC 822	Имена RFC 822 задаются в формате *имя_пользователя@имя_домена* и известны большинству пользователей как адреса электронной почты Интернета.
LDAP URL	Имена LDAP применяют именование атрибутов X.500. Они задают сервер с Active Directory и атрибуты имени объекта. Например: LDAP://servername.myco.com CN=jimsmith,OU=sys, OU=product,OU=division,O=myco,C=US
UNC	Active Directory поддерживает правила UNC, применяемые в сетях на базе Windows 2000 для обращения к доступным томам, принтерам и файлам. Например: \\servername.myco.com\xl\budget.xls.

Стандарты имен определяет интерфейс. Иногда могут быть использованы любые стандарты имен (например, при входе в систему), однако может потребоваться и специальный стандарт. Например, утилите LDP — средству поддержки Active Directory — требуются LDAP-имена.

Структура Active Directory

Active Directory предоставляет способ для разработки структуры каталога в зависимости от потребностей Вашего предприятия. Поэтому перед установкой Active Directory надо исследовать бизнес-структуру и деятельность организации.

Active Directory выделяет в сети две структуры: логическую и физическую.

Логическая структура

В логическую структуру организуют ресурсы, что позволяет искать их по именам, а не физическому расположению.

Объект

Объект (object) — это отличительный набор именованных атрибутов, описывающих сетевой ресурс. *Атрибутами* (attribute) называются характеристики объектов в каталоге. Например, атрибуты пользователя могут включать его фамилию и имя, отдел и адрес электронной почты,

В Active Directory можно организовывать объекты в *классы* (classes), логически группирующие объекты. Так, классом объекта могут быть пользователи, группы, компьютеры, домены или организационные подразделения (ОП).

Примечание *Контейнерные объекты* (container object) могут содержать другие объекты. Таковым, например, является домен.

Организационное подразделение

Это контейнерный объект для организации объектов в логические административные группы в рамках домена. ОП может содержать такие объекты, как учетные записи пользователей, группы, компьютеры, принтеры, приложения и другие ОП. Иерархия ОП в домене не зависит от структуры других доменов — каждый может поддерживать собственную иерархию.

Домен

Это основная единица логической структуры в Active Directory. Группировка объектов в один или несколько доменов позволяет отразить в сети структуру предприятия.

Все сетевые объекты существуют в пределах домена, и каждый домен хранит сведения только о содержащихся в нем объектах. Теоретически каталог домена может содержать более 10 миллионов объектов, но практически проверен и поддерживается 1 миллион.

Доступ к объектам домена регламентируется *списком управления доступом* (Access Control List, ACL), содержащим *строки контроля доступа* (Access Control Entry, ACE). Все политики безопасности и параметры одного домена, например административные разрешения и списки ACL, не пересекаются с параметрами другого. Администратор домена имеет абсолютные права на установку политик только в пределах своего домена.

Примечание Доменом называют *раздел* (partition) Active Directory. Совокупность доменов в пределах леса образует службу Active Directory.

В типичный домен входят компьютеры следующих типов.

- **Контроллеры домена под управлением Windows 2000 Server** хранят и поддерживают копию каталога. Подробности о них см. далее.
- **Рядовые серверы домена под управлением Windows 2000 Server.** *Рядовыми* (member server) называют серверы, не сконфигурированные как контроллеры домена. На таком сервере не хранится информация каталога и не выполняется авторизация пользователей. Рядовые серверы предоставляют доступ к своим ресурсам, например к папкам или принтерам.
- **Клиентские компьютеры под управлением Windows 2000 Professional** с запущенным окружением рабочего стола позволяют пользователям получать доступ к ресурсам домена.

Дерево

Это группировка или иерархия одного или нескольких доменов Windows 2000, предоставляющих совместный доступ к ресурсам. Дерево может содержать только один домен Windows 2000. Впрочем, можно создать большее непрерывное пространство имен, объединив несколько доменов в иерархическую структуру.

На рис. 1-5 **показан пример** родительского **домена** (microsoft.com) **и двух** дочерних (dev.microsoft.com **и product.microsoft.com).**

Все домены в дереве предоставляют единый доступ к информации и ресурсам. В дереве доменов только один каталог, но каждый домен предоставляет свою часть каталога, содержащую данные об учетных записях «своих» пользователей. В пределах дерева пользователь, вошедший в систему в одном домене, может обращаться к ресурсам другого в течение всего срока действия соответствующих разрешений.

Windows 2000 собирает информацию со всех доменов в один каталог, обеспечивая доступ к нему из каждого домена. Каждый домен, кроме того, автоматически создает индекс информации своего подраздела в Active Directory, хранящийся на контроллерах домена. Пользователи обращаются к этому индексу для поиска других пользователей, компьютеров, ресурсов и приложений по всему дереву доменов. Все домены в пределах дерева

обеспечивают доступ к общей *схеме* (schema) — формальному описанию объектов в хранилище Active Directory. Все домены одного дерева обеспечивают доступ к общему *глобальному каталогу* (global catalog) — центральному репозитарию информации об объектах дерева или леса.

Все домены дерева предоставляют доступ к общему пространству имен и иерархической структуре имен. *Пространство имен* (namespace) — набор правил именования, обеспечивающих иерархическую структуру, или путь дерева. По стандартам DNS имя дочернего домена дополняется именем родительского. Имя дерева доменов должно соответствовать зарегистрированному в Интернете имени предприятия.

В Active Directory деревья различают по:

- иерархии доменов;
- непрерывности пространства имен;
- доверительным отношениям Kerberos между доменами;
- общей схеме;
- способности отображать любой объект в списке глобального каталога.

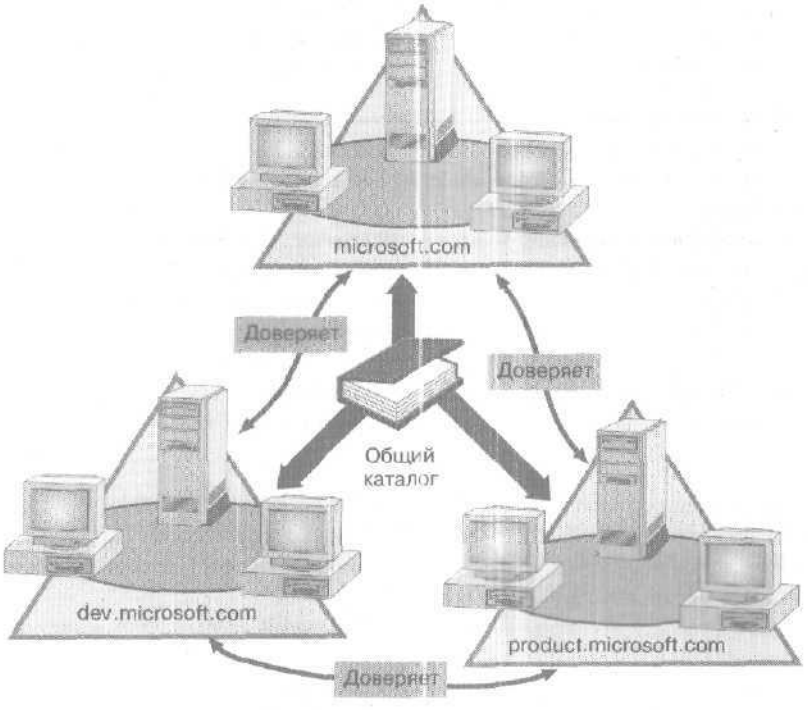


Рис. 1-5. Дерево доменов в Windows 2000

Лес

Лес — объединение одного или более деревьев — позволяет группировать подразделения предприятия (или два предприятия для объединения их сетей), которые не используют одинаковую схему именования, работают независимо друг от друга, но должны обмениваться данными.

Деревья в лесу обеспечивают доступ к одинаковой схеме и правилам совместной работы объектов. Все домены леса имеют единый глобальный каталог и конфигурационный контейнер.

Леса различаются по:

- одному или более набору деревьев;
- несвязанному пространству имен между этими деревьями;
- доверительным отношениям между деревьями по протоколу Kerberos;
- общей схеме;
- способности отображать любой объект в глобальном каталоге.

Объекты деревьев домена, образующие лес, доступны всем его пользовательским объектам. Впрочем, при доступе к объекту другого дерева пользователю надо знать его полное доменное имя или обеспечить удобный просмотр множества полных имен доменов при поиске ресурса во всей сети.

Доверительные отношения

Домены в дереве связываются друг с другом, используя двусторонние транзитивные доверительные отношения по протоколу Kerberos. *Транзитивное доверие Kerberos* (Kerberos transitive trust) означает, что если домен А доверяет домену Б и домен Б доверяет домену В, то домен А доверяет домену В. Поэтому присоединенный к дереву домен сразу вступает в доверительные отношения с каждым доменом дерева. Эти отношения делают все объекты во всех доменах дерева доступными всем прочим доменам в дереве.

Доверительные отношения — связующее звено между минимум двумя доменами, при этом доверяющий домен предоставляет аутентификацию входа в систему доверяемому. Пользовательские учетные записи и группы, определенные в доверяемом домене, могут получать права и полномочия в доверяющем, даже если их нет в его каталоге.

На рис. 1-6 показаны различия между двусторонними доверительными отношениями Windows NT и упрощенной моделью транзитивных отношений в Windows 2000.

В Windows NT 4.0 и более ранних версиях междоменные доверительные отношения определялись явными односторонними доменными учетными записями между контроллерами доменов. Каждое отношение устанавливалось и управлялось индивидуально. Управление односторонними отношениями между доменами большой сети проблематично.

Транзитивные доверительные отношения

Если двустороннее доверие неприемлемо, администратор сети может явно определить односторонние доверительные учетные записи для заданного домена. Эта возможность поддерживается для связи с существующими доменами Windows NT 4.0 и более ранних версий и позволяет устанавливать доверительные отношения с доменами в других лесах.

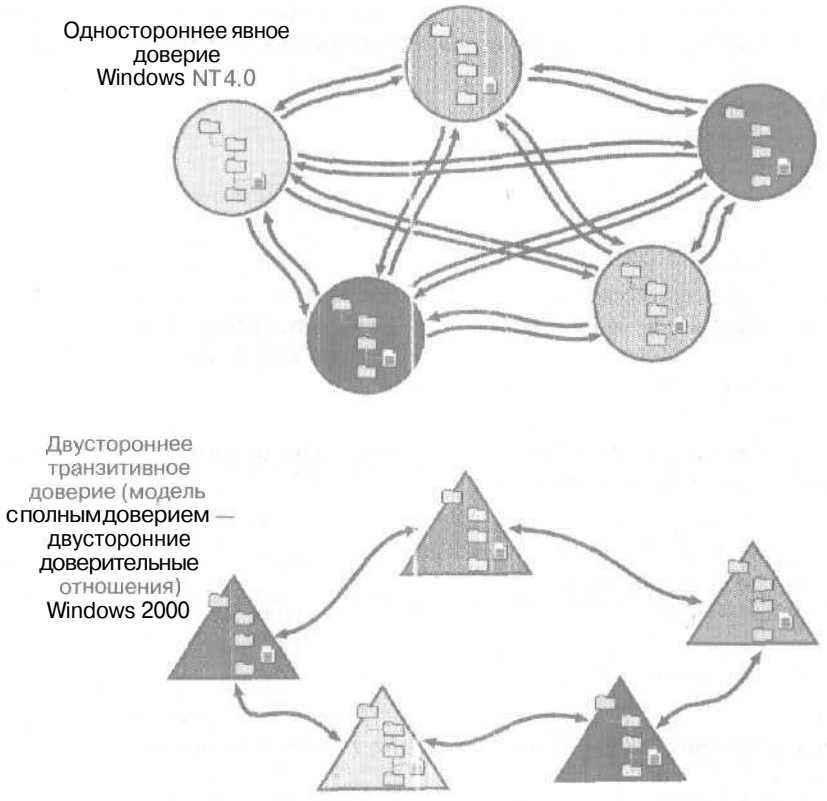


Рис. 1-6. Доверительные отношения в доменах Windows NT и Windows 2000

Доверительные отношения в Windows 2000

При включении домена в дерево доверительные отношения между новым доменом и корнем родительского домена дерева устанавливаются автоматически. Транзитивное доверие — свойство Kerberos-систем — обеспечивает распределенную аутентификацию и авторизацию (проверку подлинности) на Windows 2000-компьютерах.

Примечание Односторонние доверительные отношения можно задать в свойствах домена в оснастке Site Manager (Диспетчер сайтов). *Оснастка* (snap-in) — тип инструмента, который можно добавить в консоль, поддерживаемую MMC (см. главу 6).

Физическая структура

Физическая структура Active Directory касается эффективности репликации БД каталога между контроллерами доменов.

Контроллер домена

Это компьютер с Windows 2000 Server, хранящий реплику раздела каталога (локальная БД домена). У всех контроллеров в домене есть полная реплика доменной части каталога. При выполнении действия, повлекшего изменение каталога, Windows 2000 автоматически реплицирует обновления на все контроллеры домена. Некоторые важные изменения, скажем, смена пароля или блокирование учетной записи пользователя, сразу реплицируются по всему домену.

В домене учетная запись пользователя, которую Windows 2000 заносит в каталог, создается однократно. При входе пользователя в домен контроллер проверяет в каталоге имя пользователя, пароль и ограничения для аутентификации пользователя. Информация каталога периодически реплицируется между контроллерами домена. В качестве контроллеров могут выступать только компьютеры с Windows 2000 Server, Advanced Server или Datacenter Server.

Сайт

Концепция сайтов стала известной благодаря выпуску продуктов семейства Microsoft BackOffice. Она включена в Active Directory; впрочем, она отличается от концепции сайта в некоторых продуктах BackOffice, например, Microsoft Exchange. Главное отличие сайтов Active Directory от продуктов BackOffice в том, что сайты Active Directory определяются как диапазон IP-подсетей. В продуктах BackOffice, например, в Microsoft Exchange Server сайтом называется логическая группировка серверов, независимая от физического расположения самих серверов.

Сайт Active Directory представляет собой набор диапазонов TP-подсетей. Например, он может определяться как подсеть с диапазоном 192.168.10.0/24 — 192.168.20.0/24, в другой части ГВС — диапазоном 172.20.10.0/24 — 172.20.20.0/24. Впрочем, оба сайта могут быть частью одного и того же домена Windows 2000.

Примечание Формат /24 в предыдущем примере представляет 24 бита, которые читаются слева направо, т. е. в виде 255.255.255.0. Формат /22 соответствовал бы виду 255.255.252.0 или 22 битам, читаемым слева направо.

Одно из преимуществ Active Directory в том, что домены могут охватывать ГВС с различной топологией и местоположением и оставаться при этом «прозрачными» для пользователей. Выделяя группы локальных подсетей в сайты, администраторы могут контролировать трафик репликации между подсетями, а значит, и между сайтами. В итоге трафик в ГВС сокращается.

Идея сайта также используется клиентом при поиске контроллера домена для подтверждения полномочий на вход в систему. Пользователь одного сайта может сидеть за рабочей станцией другого сайта. Для подтверждения его полномочий необходимо найти контроллер домена пользовательского сайта. Сравнение сайтов пользователя и рабочей станции (т. е. сравнение подсетей) поможет найти соответствующий контроллер домена.

Резюме

Служба каталогов позволяет организовать и упростить доступ к ресурсам сетевых компьютерных систем. Windows 2000 поддерживает безопасное сетевое окружение, в котором пользователи получают доступ к общим ресурсам независимо от размера сети. Windows 2000 поддерживает два типа сетей: рабочие группы и домены. Windows 2000 включает службу каталогов Active Directory, обеспечивающую централизованное управление сетью. Она позволяет легко добавлять, удалять и перемешать ресурсы. Active Directory полностью отделяет логическую структуру иерархии домена от физической. Первая состоит из объектов, ОП, деревьев доменов и транзитивных доверительных отношений Kerberos, автоматически устанавливаемых между новым доменом и корнем родительского домена дерева; вторая — из контроллеров домена и сайтов.

Закрепление материала

? 1 Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сможете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Клиент попросил Вас порекомендовать подходящую серверную ОС семейства Windows 2000, исходя из следующих условий:
   - все удаленные офисы соединены со штаб-квартирой предприятия и центром обработки данных высокоскоростными (более 10 Мб/с) каналами;
   - все 10 000 пользователей используют Windows 2000 Professional или Windows 98.

   Требования к функциональности:
   - все сайты получат доступ к кластеру высокодоступного сервера с БД Microsoft SQL Server 7.0; двухсерверный кластер с 6 процессорами в каждом компьютере расширять не планируется;.
   - остальные серверы будут работать под управлением Windows 2000 с установкой Active Directory, основных файлов, служб печати и удаленного доступа к сети; на них будет установлено 1–4 процессора в зависимости от количества пользователей каждого сайта (например, небольшой удаленный сайт будет работать на однопроцессорном сервере, а на всех серверах корпоративного сайта будет по 4 процессора); на всех этих компьютерах будет установлена одна и та же редакция Windows 2000.
   - каждый домен Active Directory будет поддерживать 2 500 пользователей.

2. Почему WDM-драйверы предпочтительнее старых драйверов Windows NT?

3. Как Windows 2000 защищает исполняемые компоненты (Executive) от приложений пользовательского режима?

4. Какой компонент Executive отвечает за вытесняющую многозадачность?

5. В чем главное отличие рабочей группы от домена?

6. Каковы структура и назначение службы каталогов?

ГЛАВА 2

Установка и конфигурирование Microsoft Windows 2000 Server

В этой главе

Эта глава посвящена установке Windows 2000 Server. **Вы** узнаете, какие **сведения** надо **собрать, чтобы подготовиться к выполнению этой задачи, и что перед** этим **необходимо предпринять. Мы расскажем об** этапах **обычной установки и** способах **обновления до** Windows 2000 **Server и рассмотрим типичные проблемы.**

Прежде всего

Для изучения материалов этой главы **необходимо иметь:**

- **компьютер,** отвечающий **минимальным аппаратным требованиям, приведенным во вводной главе;**
- **установочный** компакт-диск **Windows 2000** Server.

Занятие 1. Подготовка к установке Windows 2000 Server

Перед установкой Windows 2000 Server надо собрать сведения о системе и решить, как установить эту ОС. Вы узнаете о том, что сделать до установки,

Изучив материал этого занятия, Вы сможете:

- ✓ подготовиться к установке Windows 2000 Server, предварительно определив аппаратные требования и собрав необходимую информацию.

Продолжительность занятия — около 90 минут.

Подготовка к установке

В ходе установки программа Setup попросит Вас определить способ установки и конфигурирования Windows 2000. Вы должны собрать нужную информацию. Хорошо подготовившись, Вы избежите проблем во время и после установки.

Перед установкой Windows 2000 изучите список задач в приведенной ниже таблице — в следующих разделах они обсуждаются подробнее. Сначала перед Вами стоят только первые две: Вы должны убедиться, что компьютер отвечает минимальным аппаратным требованиям, и проверить аппаратную совместимость. Остальные задачи решаются в ходе установки Windows 2000 Server, которую Вы выполните в упражнениях далее в этой главе.

Задача	
Проверьте, отвечает ли Ваш компьютер минимальным аппаратным требованиям. Например, на жестком диске должно быть минимум 2 Гб свободного пространства.	D
Проверьте совместимость всех аппаратных средств (сетевые, видео- и звуковые платы, устройства чтения компакт-дисков, платы PC и т, д.) по списку HCL.	D
Решите, как разделить жесткий диск, на котором Вы хотите установить Windows 2000 Server.	□
Выберите файловую систему, обеспечивающую требуемые функции. Выберите NTFS, если Вы не собираетесь запускать на компьютере другие ОС.	D
Выберите режим лицензирования — после установки его можно изменить.	П
Выберите тип сетевой группы (рабочая группа или домен), к которой присоединится Ваш компьютер. Если Вы присоединяетесь к домену, потребуются дополнительные данные: имена домена и созданной для Вас учетной записи. Для создания учетной записи в домене нужно иметь права администратора.	П
Решите, выполнить ли новую установку или обновить существующую версию Windows NT Server. Windows NT Workstation и Windows 9x нельзя обновить до Windows 2000 Server.	!]
Выберите способ установки: загрузочные диски, компакт-диски или через локальную сеть.	П
Выберите устанавливаемые компоненты, например Networking Services (Сетевые службы) или Microsoft Indexing Service (Служба индексирования).	□

Помимо перечисленных, Вы должны выполнить и другие задачи, о которых рассказано ниже.

Работа с DNS

При создании домена Windows 2000 должна быть запушена и сконфигурирована служба DNS. Если Вы присоединяетесь к домену, Вы должны знать его DNS-имя. Если служба DNS не запущена, она будет установлена автоматически при создании контроллера домена или соответствующем изменении роли сервера.

Регистрация информации

Вы должны также знать предыдущую ОС (если есть), имя компьютера, рабочей группы или домена (если компьютер работает в сети) и текущий IP-адрес компьютера (если в Вашей сети нет сервера DHCP или сервер DHCP не будет использоваться для динамического выделения адресов).

*Резервное **копирование** файлов*

Создайте перед установкой резервные копии текущих файлов на диске, на магнитной ленте или на другом компьютере в сети.

Разуплотнение сжатых дисков

Перед обновлением до Windows 2000 надо распаковать все тома, сжатые с помощью программ DriveSpace или DoubleSpace. Производить обновление до Windows 2000 на сжатых дисках можно, только когда для их сжатия применялось средство сжатия для файловой системы NTFS. Тома DriveSpace или DoubleSpace создаются в Windows 9x. Эту ОС нельзя обновить до Windows 2000 Server, хотя она и может сосуществовать на одном компьютере с Windows 2000 Server.

Отключение зеркального отображения дисков

Если на компьютере включено зеркальное отображение дисков, то перед запуском Setup его надо отключить — завершив установку, его можно включить снова.

Примечание Отключать зеркальное отображение дисков на аппаратном уровне для новой установки Windows 2000 не надо, так как аппаратные RAID-системы не принимаются во внимание при установке ОС.

Отключение источников бесперебойного питания

Если компьютер подключен к источнику бесперебойного питания (ИБП), перед запуском Setup надо отключить кабель, подключенный к последовательному порту. Setup пытается автоматически обнаружить устройства, подключенные к последовательным портам, и наличие устройств ИБП может это затруднить в процессе такого обнаружения.

Конфликтные приложения

Перед запуском Setup прочитайте файл Readme.doc (в корневом каталоге установочного компакт-диска Windows 2000 Server), чтобы узнать о приложениях, которые надо отключить или удалить перед установкой. Возможно, потребуется удалить сканирующие антивирусы, сетевые службы сторонних фирм или клиентское ПО.

Проверка загрузочного сектора на вирусы

Вирус в загрузочном секторе не позволит установить Windows 2000. Чтобы проверить загрузочный сектор, запустите файл Makedisk.bat в каталоге \Valueadd\3rdparty\CA_antiv на установочном компакт-диске Windows 2000 Server. Утилита Makedisk.bat создает дискету, используемую для проверки загрузочного сектора. Создав ее, загрузите с нее компьютер. Загрузочный сектор будет проверен на наличие вирусов. По завершении проверки не забудьте вынуть дискету.

Сбор материалов

- Прочитайте всю документацию, имеющую отношение к установке Windows 2000: изучите TXT- и DOC-файлы на компакт-диске Windows 2000 Server.
- Убедитесь, что у Вас есть диски с драйверами всех установленных устройств и Вы знаете параметры конфигурации аппаратных средств сторонних фирм, включая драйверы и документацию.
- Отформатируйте три 3,5-дюймовых дискеты объемом по 1, 44 Мб (если Вы собираетесь создавать загрузочные дискеты).

Внимание! Загрузочные диски Windows NT 4.0 несовместимы с Windows 2000.

Минимальные аппаратные требования

Вам должны быть известны минимальные аппаратные требования для установки и использования Windows 2000 Server, чтобы Вы могли определить, отвечает ли им Ваша система.

Компонент	Минимальные требования
Процессор	32-разрядный **Pentium 133 МГц.**
Свободное дисковое пространство	Один или больше жестких дисков, где каталог %systemroot% (по умолчанию это C:\WINNT) расположен в разделе с минимум 671 Мб свободного пространства (рекомендуется 2 Гб).
Оперативная память	64 Мб для организации сети с 1–5 клиентскими компьютерами; рекомендуется минимум 128 Мб для большинства сетевых сред.
Дисплей	Монитор VGA с разрешением 640x480 (рекомендуется 1024x768).
Устройство чтения компакт-дисков	12-скоростное или более быстрое; не требуется для установки через локальную сеть.
Дополнительные дисководы	Дисковод для 3.5-дюймовых дискет высокой плотности (если компьютер нельзя загрузить с CD-ROM-привода).
Необязательные компоненты	Мышь или другое координатное устройство. Для установки через ЛВС: сетевая плата и основанная на MS-DOS сетевая ОС, позволяющая подключиться к серверу с установочными файлами Windows 2000.

Аппаратная совместимость

Setup автоматически проверяет аппаратные средства и ПО и сообщает о возможных конфликтах. Впрочем, для успешной установки Вы должны удостовериться, что аппаратные средства компьютера совместимы с Windows 2000 Server еще до запуска установки. Проверьте для этого, есть ли Ваши аппаратные средства в списке HCL (см. файл Hcl.txt в папке Support на компакт-диске Windows 2000 Server), где перечислены все модели аппаратных средств, прошедшие *тесты на аппаратную совместимость* (Hardware Compatibility Tests, HCT). Тестирование проводится в лабораториях Windows Hardware Quality Labs (WHQL), а также некоторыми независимыми разработчиками аппаратуры. Успех установки Windows 2000 Server на компьютере, оснащенном непроверенной аппаратурой, не гарантируется.

Примечание Microsoft регулярно обновляет список HCL. Самую свежую версию этого списка см. на Web-узле Microsoft WHQL — *http://www.microsoft.com/hwtest/hc*Если этот URL недоступен, попробуйте *http://www.microsoft.com/isapi/redir.dll?prdWin2000 HCL&pver=1.* Если и это не удалось, попробуйте найти нужные сведения на узле *http://www.fnicrosqft.com* по ключевому слову «HCL».

Модель аппаратного средства считается поддерживаемой, если она перечислена в HCL и Вы используете для этого устройства драйвер, авторизованный Microsoft. Термин «неподдерживаемая» не говорит о качестве устройства или драйвера сторонней фирмы. Многие неподдерживаемые компьютеры и устройства корректно работают с Windows 2000. И все же Microsoft не предоставляет полной технической помощи в случае проблем, связанных с такой аппаратурой или ее драйверами. Если одно из устройств Вашего компьютера не входит в список HCL, свяжитесь с его изготовителем и запросите драйвер для Windows 2000, если он существует.

Разделы диска

Setup позволяет установить Windows 2000 Server в существующий раздел диска или создать новый раздел и затем установить в него Windows 2000. В ходе установки Setup исследует жесткий диск. В зависимости от состояния диска Вам будут предоставлены некоторые или все параметры разбиения:

- если на жестком диске нет разделов, нужно создать установочный раздел соответствующего размера;
- если разделы есть, но при этом хватает неразмеченного пространства, можете создать на его основе новый раздел, куда затем установите Windows 2000 Server;
- если есть достаточно большой раздел, можете установить ОС на него;
- если раздел есть, можете удалить его, а на освободившемся месте создать раздел для установки Windows 2000;
- если Вы предпринимаете какое-либо действие, которое сотрет данные, Вас попросят подтвердить выбор: при удалении раздела уничтожаются все его данные; при новой установке Windows 2000 на раздел, содержащий другую ОС, последняя будет перезаписана.

Главное, что от Вас требуется, — создать установочный раздел, хотя Вы вправе использовать Setup для создания и модификации любых разделов. После установки Windows 2000 можно использовать оснастку Disk Management (Управление дисками) для изменения структуры диска.

Определение размера установочного раздела

Программе установки Windows 2000 Server требуется загрузочный раздел объемом минимум 671 Мб — для установки всех файлов ОС Windows 2000. И все же рекомендуется создать загрузочный раздел размером не менее 2 Гб, так как на него в дальнейшем будут устанавливаться дополнительные файлы и программы, например, файл подкачки Windows 2000, утилиты ОС и пакеты обновлений. Загрузочный раздел содержит основные файлы ОС.

Системный раздел содержит файлы, нужные для загрузки Windows 2000. На компьютере с процессором Intel ОС запускается из системного раздела, т. е. Windows 2000 при загрузке компьютера ищет определенные файлы, например Ntldr, Ntdetect.com и Boot.ini в корневом каталоге, обычно на диске C: (диск 0). ОС не запустится, если системный раздел не помечен как активный.

Windows 2000 Server устанавливается на загрузочный раздел, содержащий родительский каталог ОС (по умолчанию Winnt), подкаталог \System32, ядро Windows 2000 и другие файлы, нужные для работы ОС. Если Windows 2000 Server установлена на активном разделе, он является и загрузочным, и системным.

Дисковый раздел с файлами Windows 2000 должен располагаться на несъемном жестком диске, иметь достаточно свободного места и быть отформатирован под файловыми системами NTFS (версий 4,0 NTFS 5.0), FAT16 или FAT32. Впрочем, нельзя установить Windows 2000 в раздел с FAT16 или FAT32, если он был сжат, например, утилитой Microsoft DriveSpace.

Исполнимые файлы Setup — Winnt.exe и Winnt32.exe — сообщают об ошибке, если не могут найти диск с достаточным свободным пространством (больше 671 Мб) или если на диске, указанном с ключом /t: или /tempdrive:, не хватает места. В этом случае надо освободить место на диске и вновь запустить Setup.

Примечание В Windows NT раздел всегда первоначально форматировался под FAT и лишь затем конвертировался под NTFS. В Windows 2000 можно сразу отформатировать раздел под NTFS. Это позволяет создавать разделы объемом более 4 Гб, хотя для PC-совместимых компьютеров существует ограничение размера раздела в 7,8 Гб.

Windows 2000 ищет определенные файлы в корневом каталоге активного раздела при запуске компьютера. Но Вы вправе установить Windows 2000 и на другом диске, скажем, на диске D:, если он отформатирован под совместимую файловую систему. Если Вы хотите обеспечить двухвариантную загрузку на компьютере для ОС, не поддерживающих NTFS, например Windows 98, диск C: нужно отформатировать под FAT16 или FAT32.

Если системный жесткий диск содержит разделы, управляемые BIOS, то Setup будет отображать другие файловые системы, например, *сетевую файловую систему* (network file system, NFS), чередующиеся наборы, наборы томов или зеркальные отображения как разделы неизвестного типа. Во избежание их случайного удаления, не используйте Setup для удаления неизвестных разделов.

Если Вы устанавливаете новую копию Windows 2000 в программно зеркализованном разделе, отключите зеркализацию до установки; затем ее можно будет восстановить. При обновлении Windows NT Server 3.51 или 4.0 до Windows 2000 Server разрешается оставить зеркализацию на время установки.

Чтобы использовать Windows 2000 совместно с другой ОС, например MS-DOS, Windows 3.x/9x/NT, установите Windows 2000 в отдельный раздел. Хотя Вы вправе установить Windows 2000 на один раздел с предыдущей ОС, рекомендуется устанавливать Windows 2000 в отдельный раздел, потому что Setup может перезаписать файлы в папке Program Files, установленные другими ОС.

Файловые системы

При установке Windows 2000 на неразмеченное дисковое пространство Вам предлагается выбрать файловую систему, которая будет применена для форматирования раздела. Windows 2000 поддерживает NTFS и FAT (существуют две разновидности FAT: FAT16 и FAT32).

Файловая система NTFS

Windows 2000 поддерживает NTFS — файловую систему, обладающую всеми основными возможностями FAT, расширенными функциями хранения, включая защиту и сжатие, и

лучше приспособленную для работы с большими томами. Windows 2000 и Windows NT – единственные ОС, способные обращаться к данным на локальном жестком диске, отформатированном под NTFS.

Примечание Утилиты некоторых фирм обеспечивают доступ к разделам NTFS из MS-DOS и других ОС; Microsoft их не поддерживает.

Windows 2000 использует новую, пятую версию NTFS. обладающую массой возможностей для повышения производительности и такими функциями, как квотирование дискового пространства для конкретных пользователей, шифрование файлов и точки переопределения. Последние позволяют расширить возможности файловой системы. Приложения могут перехватывать операции открытия объектов файловой системы и выполнять собственный код перед возвращением данных файла. Точки переопределения мы обсудим в главе 4. Кроме того, в NTFS 5.0 разрешается добавлять дисковое пространство к томам без перезагрузки компьютера.

Для работы NTFS требуется Windows 2000 или Windows NT. Если компьютер управляется другой ОС, она не сможет обращаться к разделам NTFS.

Используйте NTFS, если раздел Windows 2000 должен реализовывать:

- локальную защиту на уровне файла или каталога — NTFS позволяет управлять доступом к файлам и каталогам независимо от способа доступа — локально или из сети;
- сжатие диска — NTFS позволяет хранить в разделе больше данных за счет сжатия файлов;
- **квотирование** — NTFS позволяет определять квоты на дисковое пространство для конкретного пользователя;
- **шифрование** — NTFS позволяет шифровать файлы на физическом жестком диске.

Рекомендуется использовать именно NTFS — только она поддерживает службы Active Directory, позволяющие выполнять множество важных функций, включая создание доменов и организацию доменной зашиты. Но если Вам требуется двухвариантная загрузка, отформатируйте разделы под FAT16 или FAT32. Если Вы планируете сделать сервер контроллером домена, отформатируйте установочный раздел под NTFS.

Файловые системы FAT16 и FAT32

Совместимы с несколькими ОС, поэтому если Вам требуется двухвариантная загрузка, отформатируйте разделы под FAT16 или FAT32. Если при установке Вы выберете FAT и раздел на диске меньше 2048 Мб, Setup автоматически отформатирует его пол FAT16; раздел объемом более 2 Гб будет отформатирован под FAT32.

Примечание Windows 2000 поддерживает тома FAT32 любого размера, созданные Windows 95 OSR2 или Windows 98. Однако Windows 2000 способна отформатировать тома FAT32 не более 32 Гб. Это вызвано ограничениями на работу с памятью в утилитах восстановления, например Autochk.

FAT16 и FAT32 не обеспечивают многих функций NTFS, таких как защита на уровне файла. Поэтому обычно рекомендуется форматировать жесткий диск под NTFS. Единственная причина использовать FAT16 или FAT32 — необходимость двухвариантной загрузки. В этом случае под FAT16 или FAT32 надо отформатировать только системный раздел. Например, если диск C: системный, его надо отформатировать под FAT16 или FAT32, но ничто не мешает отформатировать при этом диск D: под NTFS. Впрочем, Microsoft не рекомендует применять двухвариантную загрузку на серверах.

Рекомендации по выбору файловой системы

Если системный и загрузочный разделы не совпадают, по умолчанию Windows 2000 Setup отформатирует только загрузочный раздел. Форматирование системного раздела потребует дополнительных усилий. Выбирая формат файловой системы для загрузочного раздела, руководствуйтесь следующими рекомендациями.

- Можно использовать уже отформатированный раздел. По умолчанию существующая файловая система не затрагивается, все файлы в разделе сохраняются.
- Вы вправе преобразовать существующий раздел под NTFS, чтобы использовать функции защиты Windows 2000 и другие расширения файловой системы. При этом существующие файлы сохраняются, но к преобразованному разделу можно будет получить доступ только из Windows 2000 и NT.
- Существующий раздел разрешается переформатировать под NTFS или FAT, однако все файлы в нем будут уничтожены. Решив переформатировать раздел под NTFS, не забудьте, что доступ к нему можно будет получить только из Windows 2000 и NT.
- Если загрузочный раздел меньше 2Гб или Вы хотите иметь доступ к нему из MS-DOS, Windows 3.x/9x или OS/2, выберите FAT. При этом Setup отформатирует загрузочный раздел под FAT.
- Выберите FAT в случае двухвариантной загрузки с Windows 95 OSR2/9S/NT или если необходимо, чтобы загрузочный раздел был больше 2 Гб. При этом Setup отформатирует загрузочный раздел под FAT32.
- Если Вы хотите задействовать все преимущества Windows 2000, выберите NTFS — Setup отформатирует загрузочный раздел под NTFS 5,0.

Примечание Средствами Windows 2000 нельзя преобразовать том FAT16 в том FAT32.

Ниже сравниваются файловые системы, поддерживаемые Windows 2000.

Операционная система	FAT16	FAT32	NTFS
Общая совместимость	Распознается MS-DOS, Windows 3.x, Windows 95. Windows 98, Windows NT Windows 2000 и OS/2	Распознается только Windows 95 OSR2, Windows 98, Windows NT и Windows 2000	Распознается только Windows NT и Windows 2000; под управлением другой ОС (MS-DOS, Windows 9x или OS/2) нельзя получить доступ к файлам в томе NTFS на том же компьютере
Поддерживается MS-DOS и Windows 3.x	Да	Нет	Нет
Поддерживается Windows 95 до выпуска OSR2	Да	Нет	Нет
Поддерживается Windows 95 OSR2 и Windows 98	Да	Да	Нет
Поддерживается Windows NT 3.51	Да	Нет	Да, но Windows NT 3.51 не поддерживает NTFS 5.0

(окончание)

Операционная система	FAT16	FAT32	NTFS
Поддерживается Windows NT 4.0 с установленным пакетом обновлений версии 4 и выше	Да	Нет	Да. Windows NT 4.0 поддерживает NTFS 5.0
Поддерживается Windows 2000	Да	Да	Да

Лицензирование

Windows 2000 Server поддерживает два режима лицензирования: она сервер» (Per Server) и «на рабочее место» (Per Seat). В первом случае нужное число *клиентских лицензий доступа* (Client Access Licenses, CAL) определяется, исходя из количества одновременных подключений к серверу, а во втором — отдельная лицензия нужна каждому компьютеру, обращающемуся к Windows 2000 Server.

Лицензирование «на сервер»

Подразумевает выделение клиентских лицензий для подключения к определенному серверу. Каждая лицензия разрешает одно подключение клиентского компьютера к серверу для доступа к сетевым службам. В итоге количество лицензий должно соответствовать максимальному числу единовременно подключенных к серверу компьютеров.

Такая политика лицензирования предпочтительна для небольших компаний с одним сервером и для серверов Интернета или удаленного доступа, клиентские компьютеры которых лицензировать нельзя. Лицензирование «на сервер» позволяет определить максимальное число параллельных подключений к серверу и отклонить попытки входа в систему дополнительных пользователей.

Примечание Если Вы сомневаетесь, выберите режим «на сервер», так как разрешается однократно изменить его на режим «на рабочее место» без дополнительной оплаты, дважды щелкнув значок Licensing (Лицензирование) на Control Panel. Об этом изменении не надо уведомлять Microsoft. Но обратный переход в режим «на рабочее место» невозможен.

Лицензирование «на рабочее место»

Требует отдельной клиентской лицензии для каждого клиентского компьютера, обращающегося к Windows 2000 Server для доступа к основным сетевым службам. Если клиентский компьютер лицензирован, с него разрешено обратиться к любому серверу Windows 2000 в сети предприятия. Такая политика лицензирования часто более выгодна для больших сетей, где клиентские компьютеры соединяются с несколькими серверами.

При работе со службами терминалов рекомендуется режим «на рабочее место», кроме лицензии Terminal Services Internet Connector, когда режим всегда должен быть «на сервер». Если Вы хотите использовать Terminal Services, нужно установить два компонента: Terminal Services (Службы терминалов) и Terminal Services Licensing (Лицензирование служб терминалов).

Клиентская лицензия

Дает право клиентскому компьютеру соединяться с серверами Windows 2000 для доступа к сетевым службам, общим папкам и ресурсам печати. При установке Windows 2000 Server нужно выбрать режим «на рабочее место» или «на сервер».

Клиентские лицензии не требуются для:

- анонимного или авторизованного доступа к Windows 2000 Server посредством Microsoft Internet Information Services (IIS) или приложения Web-сервера, обеспечивающего доступ к HTML-файлам по протоколу HTTP;
- соединении Telnet и FTP.

Примечание Для продуктов семейства BackOffice требуются отдельные лицензии.

Рабочие группы и домены

В ходе установки Вы должны выбрать тип сети, к которой будет присоединен компьютер. Компьютер с Windows 2000 может присоединиться к сети одного из двух типов: рабочая группа или домен.

Присоединение к рабочей группе

Назначьте компьютеру имя существующей или вновь создаваемой группы. В любом случае компьютер становится членом указанной рабочей группы, и другие пользователи увидят его в соответствующем разделе сети.

Домен и рабочая группа могут совместно использовать одно имя, однако помните:

- компьютеры рабочей группы не являются членами домена;
- компьютеры рабочей группы отображаются в Windows 2000 Explorer (Проводник) вместе с компьютерами домена.

Присоединение к домену

Мастер установки Windows 2000 предлагает присоединить Ваш компьютер к существующему домену и запрашивает его DNS-имя.

Перед присоединением к домену компьютера Windows NT или Windows 2000 надо добавить его учетную запись в базу данных домена. Только пользователи с разрешением присоединять компьютер к домену вправе создать учетную запись. По умолчанию это члены групп Administrators (Администраторы), Domain Administrators (Администраторы домена) и Account Operators (Операторы учета).

Создать учетную запись Вашего компьютера в домене можно заранее или в ходе установки, выбрав переключатель Create A Computer Account In The Domain (Добавление рабочих станций к домену). При этом также надо ввести имя полномочного пользователя и пароль. По умолчанию для этого применяется учетная запись администратора.

Примечание Вам придется предоставить реквизиты домена, даже если учетная запись Вашего компьютера была заранее создана в домене.

При присоединении компьютера к домену в сети должны быть доступны минимум один контроллер домена и один сервер DNS. Если Вы устанавливаете Windows 2000 Server как отдельный сервер без присоединения к домену, Вы сможете присоединить его к домену позже, используя вкладку Network Identification (Сетевая идентификация) диалогового окна System Properties (Свойства системы) (рис. 2-1).

Обновление и новая установка

До запуска программы Windows 2000 Server Setup Вы должны решить; обновить существующую установку Windows NT или выполнить новую установку.

Обновление (upgrading) — это процесс установки Windows 2000 Server в каталоге, содержащем определенные версии Windows NT. При этом Windows 2000 Server автоматически устанавливается в каталог текущей ОС. Обновление допускают:

- Windows NT Server 3.51;
- Windows NT Server 4.0 или Windows NT 4.0 Terminal Server.

Корпоративную версию Windows NT 4.0 Server можно обновить до Windows 2000 Advanced Server, но не до Windows 2000 Server. Windows NT Server до версии 3.51 нельзя напрямую обновить до Windows 2000 Server — сначала придется обновить ее до Windows NT Server 3,51 или 4.0. Windows NT Workstation и Windows 2000 Professional также нельзя обновить до Windows 2000 Server.

Рис. 2-1. Вкладка Network Identification (Сетевая идентификация) диалогового окна System Properties (Свойства системы)

Установка (installing) в отличие от обновления подразумевает размещение ОС в новом каталоге или установку ОС на диске или дисковом разделе, где ранее не была установлена другая ОС. Если Вы хотите выполнить новую установку на раздел диска, содержащий нужные Вам приложения, придется сделать их резервную копию и переустановить после установки Windows 2000 Server.

Если Вы хотите выполнить новую установку Windows 2000 Server на раздел, ранее содержавший Windows 2000 Server, и в папке My Documents (Мои документы) хранятся нужные Вам файлы, скопируйте их в каталог Documents and Settings и верните их обратно по завершении установки. По умолчанию ярлык My Documents указывает на подкаталоги каталога Documents and Settings.

Способы установки

Существует три способа установки Windows 2000 Server на платформе Intel:

- с загрузочных дискет;
- с компакт-диска;
- по сети.

Установка при загрузке компьютера с дискет

Windows 2000 Server распространяется на компакт-диске и включает четыре загрузочных дискеты. Дискеты требуются для установки Windows 2000 Server на компьютер с процессором x86, на котором нет ОС MS-DOS или Windows и который не поддерживает загрузку с компакт-диска. Дискеты также позволяют запустить Windows 2000 после сбоя для проведения диагностики и восстановления системы.

Для создания набора загрузочных дискет запустите программу Makeboot.exe или Makebt32.exe из каталога \Bootdisk на установочном компакт-диске Windows 2000 Server. Makeboot.exe — 16-разрядное приложение, выполняемое под MS-DOS и 16-разрядными ОС вроде Windows 3.11 или Windows 9x. Makebt32.exe — 32-разрядное приложение, выполняемое под Windows NT и Windows 2000.

После начальной загрузки запускается Windows 2000, и остальная установка выполняется под Windows 2000, что удобно для выявления неполадок, поскольку при возникновении ошибки указывается ее стандартный код.

Для установки Windows 2000 Server с загрузочных дискет сначала надо выключить компьютер, вставить дискету, помеченную Windows 2000 Setup Boot Disk, и включить компьютер — установка запустится автоматически.

Примечание Для установки Windows 2000 Server на компьютер без ОС с загрузочной дискеты MS-DOS (при сетевой установке) нужно сначала отформатировать диск этого компьютера. Впрочем, установочные дискеты Windows 2000 позволяют отформатировать жесткий диск компьютера прямо в ходе установки.

Во время загрузки с дискет внизу экрана перечисляются загружаемые компоненты Windows 2000. Они описаны в следующих разделах.

Установочная дискета №1

Файл Setupldr.bin начинает установку: обследует компьютер, собирает идентификационные данные машины. Если для жесткого диска, содержащего загрузочный раздел, автоматически подобрать драйвер нельзя, загрузите драйвер сторонней фирмы. Для загрузки драйвера контроллеров SCSI или RAID сторонней фирмы следуйте инструкциям Setup. После загрузки файлов в текстовом режиме файл Ntkrnlmp.exe загружает исполняемые файлы Windows 2000.

Установочная дискета №2

Загружает HAL, средства конфигурации, шрифты, национальные параметры представления информации, драйверы и контроллеры.

Установочная дискета №3

Загружает драйверы дисковых контроллеров. При этом Setup выбирает соответствующие драйверы для системы и загружает средства поддержки динамических томов (dmboot1).

Установочная дискета №4

Загружает драйверы дисковода для гибких дисков, SCSI-устройств (привода CD-ROM, дисководов для гибких и жестких дисков) и драйверы файловых систем (FAT, NTFS и CDFS). К этому моменту Windows 2000 загружена и берет контроль над процессом установки. Открывается окно приветствия, где Вам предлагается установить Windows 2000, восстановить существующую версию Windows 2000 или прервать установку. Затем Setup пытается найти предыдущие версии Windows и существующие разделы. Вы вправе удалить существующие разделы либо создать новые. После конфигурирования разделов надо выбрать файловую систему — NTFS или FAT. По завершении форматирования раздела

начинается копирование файлов, и затем компьютер перезагружается. Перед перезагрузкой выньте дискету из дисковода.

Завершение установки

После перезагрузки установка продолжается в графическом режиме. Файлы с компакт-диска продолжают копироваться на жесткий диск. Setup обнаруживает и устанавливает устройства, а затем предлагает выбрать устанавливаемые компоненты. Выберите тип сетевой установки (обычная или выборочная) и тип сети, к которой следует присоединиться (рабочая группа или домен). Setup составляет список нужных файлов, устанавливает и конфигурирует компоненты.

Установка при загрузке компьютера с компакт-диска

Если установочные файлы Windows 2000 Server находятся на компакт-диске и BIOS Вашего компьютера поддерживает загрузку с компакт-диска, вставьте компакт-диск Windows 2000 Server в привод CD-ROM и выключите компьютер. Когда Вы снова включите его, установка начнется автоматически.

Когда Setup предложит удалить компакт-диск из привода, сделайте это, иначе при следующей загрузке установка начнется снова.

Внимание! Даже если компьютер поддерживает загрузку с компакт-диска, Вам может потребоваться настроить BIOS.

Если компьютер управляется Windows 9x или Windows NT, при вставке установочного компакт-диска Windows 2000 откроется окно мастера установки Windows 2000 (если Вы не отключили функцию автоматического запуска компакт-диска).

Сетевая установка

Скопируйте установочный компакт-диск Windows 2000 или хотя бы исходный каталог (\I386) в каталог на жестком диске сетевого сервера и откройте к нему совместный доступ. Создание общих папок мы подробно обсудим в главе 3.

Обновление Windows 95, Windows 98 и Windows NT

Если на компьютере запушена Windows 9x/NT, найдите установочные файлы в сети и запустите (двойным щелчком) программу Winnt32.exe, расположенную в каталоге I386. До Windows 2000 Server разрешается обновить только Windows NT Server — другие ОС семейства Windows нельзя обновить до Windows 2000 Server. При установке Windows 2000 Server на компьютере с Windows NT Server предлагается выбрать один из двух вариантов: Upgrade to Windows 2000 Server (Обновление до Windows 2000) или Install Windows 2000 Server (Установка новой копии Windows 2000). В остальных случаях предлагается только установить Windows 2000 Server.

В ходе обновления Windows NT Server сохраняется большинство системных параметров, личные предпочтения и установленные приложения. Если нужно организовать двухвариантную загрузку, выберите Install Windows 2000 Server и нажмите клавишу Enter или щелкните кнопку Next (Далее).

Установка новой или обновление текущей версии

Если на компьютере нет Windows 9x/NT, для подключения к общей сетевой папке с установочными файлами надо запустить MS-DOS и соответствующий сетевой клиент. Затем найдите в сети установочные файлы и запустите Winnt.exe.

Для запуска Setup на MS-DOS-компьютере требуется 500 Кб свободной базовой памяти. Удостоверьтесь, что программа Emm386.exe и все драйверы устройств загружены в верхнюю память.

Совет Для загрузки Winnt.exe в верхнюю память выполните команду LoadHigh Winnt.exe. Запустите Smartdrv.exe, иначе установка будет выполняться медленно и займет от 4 до 12 часов.

Выбор устанавливаемых компонентов

В Windows 2000 Server входят разнообразные компоненты, включая ряд средств администрирования, устанавливаемых автоматически. Кроме того, Вы вправе установить дополнительные компоненты, расширяющие функциональные возможности Windows 2000 Server. Это можно сделать в процессе установки или позже с помощью программы Add/Remove Programs, щелкнув кнопку Add/Remove Windows Components (Добавление и удаление компонентов Windows).

Выбор любого из этих компонентов обеспечивает дополнительные возможности сервера, однако устанавливать следует только действительно нужные, так как каждый из них требует дополнительного дискового пространства. Вам доступны:

Возможная серверная функция	Необязательные компоненты для установки
Сервер DHCP, DNS или WINS (в сети TCP/IP)	DHCP, DNS или Windows Internet Name Service (WINS) — из состава Networking Services (Сетевые службы)
Централизованное администрирование сети	Management and Monitoring Tools (Средства управления и наблюдения), Remote Installation Services (Службы удаленной установки)
Проверка подлинности и безопасная связь	Internet Authentication Services (Служба проверки подлинности в Интернете, из состава Networking Services), Certificate Services (Службы сертификации)
Печать	Other Network File and Print Services (Другие службы доступа к файлам и принтерам в сети), включая поддержку NetWare, Macintosh и UNIX
Службы терминалов	Terminal Services (Службы терминалов), Terminal Services Licensing (Лицензирование служб терминалов)
Доступ к файлам	Microsoft Indexing Service (Служба индексирования). Remote Storage (Внешнее хранилище), Other Network File and Print Services (Другие службы доступа к файлам и принтерам в сети), включая поддержку для NetWare, Macintosh и UNIX; для взаимодействия с компьютерами NetWare применяется Gateway Services for NetWare GSNW); средство Directory Service Migration Tool устанавливает GSNW, если не установлена служба каталогов NetWare (NetWare Directory Service, NDS)
Поддержка приложений	Message Queuing Services (Службы очереди сообщений), Quality of Service (QoS) Admission Control Service (Служба контроля допуска (QoS) из состава Networking Services)
Инфраструктура Интернета (Web)	Internet Information Services (IIS), Site Server и Lightweight Directory Access Protocol (из состава Networking Services)

(окончание)

Возможная серверная функция	Необязательные компоненты для установки
Поддержка телефона и факса	Connection Manager Administration Kit и Connection Point Services (Компоненты диспетчера подключений, из состава Management and Monitoring Tools)
Мультимедийные коммуникации	Windows Media Services (Службы Windows Media)
Поддержка разных клиентских ОС	Other Network File и Print Services (Другие службы доступа к файлам и принтерам в сети), включая поддержку NetWare, Macintosh и UNIX

Ниже описаны все необязательные компоненты. Чтобы выбрать нужные компоненты, используйте эту таблицу вместе с предыдущей.

Необязательный компонент	Описание
Certificate Services (Службы сертификации)	Поддерживают аутентификацию, включая безопасную электронную почту, аутентификацию на основе Web и аутентификацию смарт-карт.
Internet Information Services (US)	Поддерживает создание Web-узлов, конфигурирование и управление по протоколам NNTP, FTP и SMTP.
Management and Network Monitoring Tools (Средства управления и наблюдения)	Предоставляет инструменты для управления и мониторинга производительности сети, включая анализатор пакетов и протокол SNMP, Другие инструменты управления поддерживают клиентский дозвон, обновление телефонных книг клиента и утилиту для перехода от NDS к Active Directory.
Message Queuing Services (Службы очереди сообщений)	Предоставляет службы передачи сообщений, необходимые распределенным приложениям для работы в разнородных сетях или когда компьютер временно недоступен в сети.
Microsoft Indexing Service (Службаиндексирования)	Предоставляет функции индексирования документов, хранящихся на диске, позволяя искать документ по его содержанию, тексту или свойствам.
Microsoft Script Debugger (Отладчик сценариев)	Поддерживает разработку сценариев.
Networking Services (Сетевые службы)	Поддерживает работу в сети и включает: COM Internet Services Proxy (Прокси COM-служб Интернета) — поддерживает распределенные приложения, использующие протокол HTTP для связи через IIS; Domain Name System (DNS) — транслирует имена для клиентов Windows 2000, что позволяет получить доступ к серверу по имени вместо использования трудных для запоминания IP-адресов; Dynamic Host Configuration Protocol (DHCP) — позволяет серверу динамически выделять IP-адреса для других серверов в сети; исключает ручную настройку статических IP-адресов на любых серверах интрасети;

(окончание)

Необязательный компонент	Описание
	Internet Authentication Service (Служба проверки подлинности в Интернете) — аутентифицирует пользователей, подключенных по телефонной линии; QoS Admission Control Service (Служба контроля допуска QoS) — позволяет контролировать распределение пропускной способности сети между приложениями; важным приложениям предоставляется наибольшая часть емкости канала; Simple TCP/IP Services (Простые службы TCP/IP) — поддерживает такие службы, как Character Generator, Day-time Discard, Echo и Quote of the Day; Site Server ILS Service (Службы ILS сервера сайта) — поддерживает приложения телефонии, обеспечивающие доступ к таким функциям, как определение номера (AOH), конференции, проведение видеоконференций и работу с факсами; поддержка зависит от IIS; WINS — обеспечивает разрешение имен NetBIOS поверх TCP/IP для клиентов Windows NT и ранних версий ОС Microsoft, в результате чего пользователи могут получать доступ к серверам по имени, а не по трудным для запоминания IP-адресам. **Примечание** Каталог Clients на установочном компакт-диске Windows 2000 Server включает два подкаталога: WIN9X содержит клиент службы каталогов для Windows 9x, а WIN9XIPP.CLI — клиент печати через Интернет для Windows 9x.
Other Network File and Services (Другие службы доступа к файлам и принтерам в сети)	Включает службы доступа к файлам и принтерам для Macintosh и службы печати для UNIX.
Remote Installation Services (Службы удаленной установки)	Предоставляет службы для удаленной установки Windows 2000 Professional на клиентские компьютеры. Клиенты должны поддерживать удаленную загрузку. На сервере для этих служб нужен отдельный раздел.
Remote Storage (Внешнее хранилище)	Обеспечивает расширение дискового пространства за счет повышения доступности сменных носителей, например магнитных лент. Редко используемые данные переносятся на ленту и при необходимости восстанавливаются.
Terminal Services Licensing (Лицензирование служб терминалов)	Предоставляет лицензии клиентам служб терминалов.
Windows Media Services (Службы Windows Media)	Позволяет передавать потоки мультимедиа через интрасеть или Интернет.

(*окончание*)

Необязательный компонент	Описание
Terminal Services (Службы терминалов)	Обеспечивает выполнение клиентских приложений на сервере, когда клиентские компьютеры функционируют как терминалы. Сервер обеспечивает многосеансовую среду и выполняет Windows-программы, используемые клиентами. Устанавливая Terminal Services, Вы должны установить и Terminal Services Licensing, чтобы лицензировать клиентов Terminal Services. Впрочем, клиентам могут быть предоставлены временные (на 90 дней) лицензии на использование сервера терминалов.

Резюме

Перед установкой Windows 2000 Server надо собрать сведения о системе и решить, как устанавливать ОС: с загрузочных дискет, с компакт-диска или по сети. Убедитесь, что компьютер отвечает минимальным аппаратным требованиям и проверьте совместимость аппаратуры с Windows 2000. Вы должны определить, как поделить жесткий диск на разделы и какую файловую систему использовать на каждом из них. Вам надо выбрать режим лицензирования, тип сети, к которой будет присоединен сервер, и дополнительные компоненты.

Занятие 2, Установка Windows 2000 Server

Это занятие посвящено выполнению новой установки Windows 2000 Server. Мы обсудим установочные программы и опишем этапы процесса установки.

Изучив материал этого занятия, Вы сможете:

- ✓ определить, какую программу использовать для установки Windows 2000 Server;
- ✓ описать три этапа процесса установки;
- ✓ выполнить новую установку Windows 2000 Server.

Продолжительность занятия — около 30 минут.

Программы установки Windows 2000 Server

Независимо от способа установки Windows 2000 Server Вы должны запустить Winnt.exe либо Winnt32.exe. Эти программы можно запустить с помощью Setup.exe. Для установки из MS-DOS или Windows 3.x запустите Winnt.exe из командной строки MS-DOS. Для установки из Windows 9x или Windows NT Workstation запустите Winnt32.exe. Для установки или обновления из Windows NT Server 3.51 или 4.0 применяется Winnt32.exe. Winnt.exe или Winnt32.exe можно вызвать с разными ключами для настройки способа установки.

Программа установки Windows 2000

Setup.exe — программа установки Windows 2000 — расположена в корневом каталоге установочного компакт-диска Windows 2000 Server. При ее запуске открывается окно Microsoft Windows 2000 CD (Компакт-диск Microsoft Windows 2000), где Вам предлагается установить Windows 2000 Server, дополнительные компоненты, просмотреть содержимое компакт-диска или выйти из Setup. Щелчок пункта Install Windows (Установка Windows) запускает Winnt.exe или Winnt32.exe в зависимости от действующей в данный момент ОС.

Окно Windows 2000 CD автоматически откроется после вставки установочного компакт-диска в привод CD-ROM, если в системе включена функция автозапуска; файл Autorun.inf вызывает программу Setup exe, которая проверяет версию ОС. Если Setup определит, что компьютер работает под Windows NT Server 3.51/4.0 или более ранней версии Windows 2000 Server, Вам будет предложено обновить или заново установить Windows 2000. Если на компьютере установлена более новая версия Windows 2000 Server, установка будет прервана.

Программа Winnt.exe

Обычно применяется для сетевой установки, в ходе которой используется сетевой клиент MS-DOS. Winnt.exe;

1. создает временный каталог WIN_NT.~BT на системном разделе и копирует в него установочные файлы;
2. создает временный каталог WIN_NT.~LS и копирует в него с сервера файлы Windows 2000;
3. предлагает пользователю перезагрузить систему, после чего выводит меню загрузки, и установка продолжается.

Winnt.exe устанавливает Windows 2000 Server и запускается из командной строки MS-DOS или 16-разрядной ОС Windows.

Ключи Winnt.exe

Для настройки работы программы Winnt.exe применяются ключи:

```
WINNT [/s[:исходный_путь]] [/t[:рабочий_диск]] [/u[:файл_ответов]]
[ /udf:id [,файл_UDF]] [/r:папка] [/rx:папка] [/e:команда] [/a]
```

Вот их подробное описание:

Ключ	Описание
/s[:*исходный_путь*]	Указывает расположение исходных файлов Windows 2000 — полный путь вида x:[*путь*] или допустимое UNC-имя.
/t[:*рабочий_диск*]	Задает диск для размещения временных файлов установки и для размещения устанавливаемой системы Windows 2000. Если диск не указан, программа установки попытается самостоятельно назначить рабочий диск.
/u[:*файл_ответов*]	Задает автоматическую установку с использованием файла ответов (требуется указать параметр /s). Файл ответов содержит ответы на некоторые или все запросы программы установки. Обычно эти ответы дает конечный пользователь.
/udf:id [,*файл_UDF*]	Указывает идентификатор (ID), используемый Winnt.exe, чтобы определить, как UDF-файл будет изменять параметры файла ответов (см. параметр /и). Параметр /udf перекрывает значения файла ответов, а идентификатор указывает, какие значения UDF-файла будут использованы. Если UDF-файл не указан, Winnt.exe запросит дискету с файлом $Unique$.udb.
/r[:*папка*]	Задает необязательную папку для установки. Папка остается по окончании установки.
/rx[:*папка*]	Задает необязательную папку для копирования. Папка удаляется по окончании установки.
/e	Задает выполнение указанной команды по окончании графической части установки.
/a	Специальные возможности для людей с плохим зрением.

Программа Winnt32.exe

Применяется для установки Windows 2000 Server из Windows 9x/NT. Запускается двойным щелчком значка Winnt32.exe в каталоге \I386 на установочном компакт-диске Windows 2000 Server или, при сетевой установке, в общем сетевом каталоге. Для указания ключей можно запустить Winnt32.exe, выбрав в меню Start (Пуск) команду Run (Выполнить) либо выполнив команду Winnt32 из командной строки Windows 9x/NT.

Если установка Windows 2000 Server запущена по сети, Winnt32.exe создает временный каталог WIN_NT.~LS и копирует файлы Windows 2000 Server с сервера в этот каталог. Временный каталог создается в первом разделе достаточного объема, если иное не задано ключом /t.

Ключи WINNT32.EXE

Для настройки работы программы Winnt32.exe применяются ключи:

```
winnt32 [/s:исходный_путь][/tempdrive:буква_диска]
[unattend[num]:[файл_ответов]]
```

[/copydir:*папка*] [/copysource:*папка*]
[/cmd:*командная_строка*] [/debug[*уровень*]:[*имя_файла*]]
[/udf:*код*[,*файл_UDF*]] [/syspart :*буква_диска*] [/checkupgradeonly]
[/cmdcons] [/m:*папка*] [/makelocalsource] [/noreboot]

Вот их подробное описание:

Ключ	Описание
/tempdrive: *буква_диска*	Назначает размещение временных файлов в заданном разделе и установку в нем Windows 2000.
/cmdcons	Добавляет консоль восстановления на экран выбора ОС для восстановления установки, завершившейся неудачей. Используется только после установки.
/s: исходный_путь	Задает размещение источника устанавливаемых файлов Windows 2000. Для копирования файлов с нескольких серверов следует указать несколько ресурсов /s. Если используется несколько ключей /s, первый из указанных серверов должен быть доступен; иначе команда не будет выполнена.
/unattend или /u	Обновляет предыдущую версию Windows 2000, Windows NT 3.51/4.0, Windows 98/95 без вмешательства пользователя. Все настройки, сделанные пользователем, считываются из файлов текущей версии системы. Ключ /unattend подтверждает, что пользователь прочитал и согласился с лицензионным соглашением для Windows 2000. Прежде чем задать этот ключ для установки Windows 2000 от лица другой организации, надо подтвердить, что конечный пользователь (физическое или юридическое лицо) получил и принял условия соглашения. Изготовители компьютеров не могут применять этот ключ на компьютерах, продаваемых конечным пользователям.
/unattend[*пит*] [:*файл_ответов*]	Выполняет чистую установку без вмешательства пользователя. Файл ответов содержит особые спецификации. Параметр *пит* задает количество секунд с момента окончания копирования файлов программой установки до момента перезагрузки компьютера. Параметр *пит* можно использовать на любом компьютере с системами Windows NT/2000. Параметр *файл_ответов* задает имя файла ответов.
/copydir:*папка*	Создает дополнительную папку внутри папки, куда устанавливаются файлы Windows 2000. Например, если в каталоге источника имеется подкаталог с именем Личные_драйверы, содержащий нужные версии драйверов, для копирования этого подкаталога в каталог установки Windows 2000 можно применить команду /copydir:Личные_драйверы. Путь к новой папке будет выглядеть так: C:\Winnt\Личные_драйверы. Команда /copydir позволяет создать любое необходимое количество дополнительных папок.
/cmd:*командная_строка*	Указывает Winnt32.exe выполнить указанную команду перед завершающей фазой установки. Это происходит после двух перезагрузок компьютера и после сбора Winnt32.exe сведений о конфигурации, но перед завершением установки.

(окончание)

Ключ	Описание
/copysource:*папка*	Создает временную дополнительную папку в папке, куда устанавливаются файлы Windows 2000. Например, если в каталоге источника есть подкаталог Личные_драйверы с нужными версиями драйверов, для копирования этого подкаталога в каталог установки Windows 2000 и использования содержащихся в нем файлов во время установки можно дать команду /copysource:Личные_драйверы. При этом путь к новой папке будет выглядеть так: C:\Winnt \Личные_драйверы. В отличие от папок, созданных командой /copydir, папки, созданные командой /copysource, удаляются по завершении программы установки.
/debug *[уровень]* [:*имя_файла*]	Создание журнала отладки на заданном уровне, например /debug4:C:\Win2000.log. По умолчанию создается файл журнала C:\%Windir%\Winnt32. log с уровнем отладки, равным 2. Уровни журнала имеют следующие значения: 0 — серьезные ошибки, 1 — ошибки, 2 — предупреждения, 3 — сообщения и 4 — подробные сообщения для отладки. Каждый уровень включает все уровни, расположенные ниже,
/udf:*код* [,*файл_UDF*]	Задает идентификатор (код), который Winnt32.exe использует для указания способа изменения файла ответов файлом БД уникальности Uniqueness Database (UDB); см. описание ключа /unattend. Параметр UDB изменяет значения в файле ответов, а идентификатор определяет используемые в файле UDB значения. Например, команда /udf: Пользователь_RAS, Наша_организация.udb заменяет параметры для идентификатора *Пользователь_RAS* в файле *Наша_организация.udb*. Если файл UDB не указан, Winnt32.exe запросит диск, содержащий файл $Unique$.udb.
/checkupgradeonly	Проверяет компьютер на совместимость по обновлению с Windows 2000. Для обновления Windows 95/9S программа установки создает файл отчета Upgrade.txt в папке, в которую устанавливается Windows. При *обновлении* Windows NT 3.51 или 4.0 отчет сохраняется в файле Winnt32.log в установочной папке.
/syspart:*буква_диска*	Указывает Setup скопировать загрузочные файлы на жесткий диск, пометить диск как активный и установить диск на другом компьютере. Когда этот компьютер запускается, он автоматически переходит на следующую фазу установки. Параметр /syspart всегда следует использовать вместе с параметром /tempdrive. Параметр /syspart для Winnt32.exe используется только на компьютерах с Windows NT 3.51/ NT 4.0 или Windows 2000. В системах Windows 9x он не предусмотрен.
/m:*папка*	Указывает копирование Winnt32.exe файлов замены из альтернативной папки. Winnt32.exe ищет файлы сначала в альтернативной папке и, если находит их, обращается к ее файлам, а не к содержащимся в папке, используемой по умолчанию.
/makelocalsource	Указывает программе установки копировать все исходные файлы установки на локальный жесткий диск. Эту команду следует использовать в случае установки с компакт-диска, чтобы создать копии установочных файлов для продолжения установки при отсутствии доступа к компакт-диску.
/noreboot	Указывает Winnt32.exe не перезапускать компьютер после завершения фазы копирования файлов. Это позволяет выполнить другую команду.

Процесс установки

Процесс установки Windows 2000 Server включает три этапа: предварительное копирование, текстовый режим и графический режим.

Предварительное копирование

Все нужные для установки файлы копируются во временные каталоги на локальном жестком диске. После ввода команды Winnt.exe или Winnt32.exe для запуска сетевой установки, все необходимые файлы копируются по сети во временный каталог WIN_NT.~LS. Затем установка продолжается, как если бы Вы устанавливали ОС с локального диска, переходя к этапу текстового режима и затем к графическому этапу.

Вы вправе не создавать загрузочные дискеты, пометив флажок Copy All Setup Files From The Setup CD To The Hard Drive (Копировать все файлы с CD-ROM на жесткий диск) под кнопкой Advanced Options (Дополнительные параметры). В этом случае каталог WIN_NT.~BT создается на диске. Этот каталог содержит файлы, которые в противном случае были бы размешены на четырех загрузочных дискетах.

Копирование файлов в каталог WIN_NT.~LS не требует остановки Windows 95/98/NT. Это ускоряет обновление.

Текстовый режим

Setup запрашивает у Вас информацию, необходимую для установки. **После** принятия лицензионного соглашения надо указать или создать установочный раздел и выбрать для него файловую систему. Затем файлы копируются из временного каталога (или с компакт-диска) в установочный каталог на жестком диске.

Лицензионное соглашение Windows 2000 Server

Лицензионное соглашение занимает несколько страниц. Прочитав его, нажмите клавишу F8, чтобы принять его условия.

Имеющиеся установки Windows

Если Setup обнаруживает и отображает перечень существующих установок Windows 2000, Вы можете выбрать установку из списка и, нажав клавишу R, восстановить ее или, нажав Esc, продолжить новую установку.

Разделы

Setup отображает все существующие разделы и свободное пространство в системе. Используя клавиши-стрелки «вверх» и «вниз», можно выбрать раздел, куда будет установлена Windows 2000 Server. Вы также вправе создавать и удалять разделы. Нажмите клавишу Enter для продолжения.

Файловые системы

Setup предлагает сохранить текущую файловую систему неизменной или преобразовать ее в NTFS. Если Вы не хотите менять текущую файловую систему, выберите Leave Current file system Intact (Оставить текущую файловую систему без изменений) (по умолчанию) и нажмите клавишу Enter для продолжения.

Setup исследует жесткие диски и копирует нужные для установки файлы из временного каталога в установочный каталог (по умолчанию это Winnt).

Графический режим

После перезагрузки компьютера установка продолжается в графическом режиме. На этом этапе Вам предлагается выбрать необязательные компоненты для установки и назначить пароль администратора.

Графический режим включает три стадии:

- сбор информации о компьютере;
- установку сетевых средств;
- завершение установки.

Сбор информации о компьютере

Для сбора информации о конфигурации для настройки системы применяется несколько диалоговых окон. На этом этапе устанавливаются функции защиты Windows 2000, устанавливаются и конфигурируются устройства.

Региональные настройки

Windows 2000 отображает текущие (заданные по умолчанию) региональные параметры. Вы также можете установить поддержку дополнительных языков, изменить представление чисел и дат и задать стандартные параметры учетных записей пользователя.

Реквизиты пользователя

При конфигурировании системы Вы должны ввести имя, на которое зарегистрирована Windows 2000 Server. Можно указать и название Вашей организации, хотя это и необязательно.

Режим лицензирования

Вы должны выбрать способ лицензирования: «на сервер» или «на рабочее место». В первом случае надо ввести номер серверной лицензии.

Имя компьютера и пароль администратора

Вы должны ввести имя компьютера (имя NetBIOS до 15 символов). Заметьте: автоматически сгенерированное имя имеет длину 15 символов. Имя, которое Вы вводите, должно отличаться от имени другого компьютера, рабочей группы или домена в сети. Вы можете использовать стандартное имя или ввести другое.

Вам будет предложено ввести пароль для локальной учетной записи Administrator (Администратор). Пароль может иметь длину до 127 символов, хотя его можно оставить и пустым.

Мастер компонентов Windows

Позволяет добавлять и удалять дополнительные компоненты в ходе и после установки. Эти компоненты описаны в занятии 1 этой главы.

Настройка даты и времени

В ходе установки Вам будет предложено выбрать часовой пояс и скорректировать дату и время.

Установка сетевых средств

По завершении сбора информации о компьютере Setup вновь выводит окно Windows, 2000 Setup. Затем компьютер исследуется в поисках сетевых плат. Это может занять несколько минут.

Настройка сетевых параметров

В ходе установки сетевых средств Вам предлагается выбрать тип установки: обычная (по умолчанию) или выборочная. В первом случае устанавливаются все стандартные компоненты: Client for Microsoft Networks (Клиент для сетей Microsoft), File and Print Sharing for Microsoft Networks (Служба доступа к файлам и принтерам сетей Microsoft) и Internet Protocol (TCP/IP) (Протокол Интернета) сконфигурированный как клиент DHCP.

Выборочная установка позволяет сконфигурировать следующие компоненты.

- **Клиенты** — по умолчанию устанавливается Client For Microsoft Networks. Вы можете добавить Gateway (and Client) Services for NetWare [Службы шлюза (и клиента) для NetWare].
- **Службы** — по умолчанию устанавливается File and Printer Sharing for Microsoft Networks. Вы можете добавить SAP Agent (Агент SAP) и QoS Packet Scheduler (Планировщик пакетов QoS), а также изменить параметры File and Printer Sharing for Microsoft Networks, выделив эту службу и шелкнув кнопку Properties (Свойства). Это позволяет оптимизировать работу службы и обеспечить совместимость с клиентами LAN Manager 2.x.
- Протоколы — по умолчанию устанавливается Internet Protocol (TCP/IP). Вы можете добавить дополнительные протоколы, включая NWLink IPX/SPX, NetBEUI, DLC, AppleTalk, Network Monitor Driver и др. Вы вправе настраивать параметры протокола, выделив его и щелкнув кнопку Properties (Свойства).

Завершение установки

На этом этапе участия пользователя не требуется. Ниже приведен краткий обзор задач, выполняемых программой Setup.

Задача	Описание
Копирование файлов	Копируются все остальные необходимые для завершения установки файлы, например стандартные программы и растровые рисунки.
Конфигурирование компьютера	Формируются меню Start (Пуск), группы программ, устанавливаются спулер печати, принтеры, службы, учетная запись администратора, шрифты, файл подкачки и регистрируется множество DLL-файлов.
Сохранение конфигурации	Сохраняется конфигурация в системном реестре, создается каталог восстановления и инициализируется Boot.ini.
Удаление временных файлов	Удаляются временные файлы и каталоги, созданные и использованные в ходе установки, например каталог WIN_NT.~LS; в реестре сжимаются системные *кусты* (hives).

Упражнение 1: установка Windows 2000 Server

Вы установите Windows 2000 Server на компьютер без отформатированных разделов. При этом с помощью программы установки Windows 2000 Server Вы создадите на жестком диске раздел, куда будет установлена Windows 2000 Server как отдельный сервер в рабочей группе.

► Задание 1: создайте установочные дискеты Windows 2000 Server

Выполните эту процедуру на компьютере под управлением MS-DOS или любой версии Windows, с которого можно получить доступ к каталогу Bootdisk на установочном компакт-диске Windows 2000 Server.

Если Ваш компьютер способен загружаться с компакт-диска, можно установить Windows 2000 без установочных дисков. Для выполнения упражнения отключите функцию загрузки с компакт-диска в BIOS.

Внимание! Вам потребуется четыре отформатированных дискеты емкостью 1,44 Мб. Учтите: данные на этих дискетах будут перезаписаны без предупреждения.

1. Пометьте четыре отформатированные дискеты следующим образом:

   Установочная дискета Windows 2000 Server № 1;

   Установочная дискета Windows 2000 Server №2;

   Установочная дискета Windows 2000 Server №3;

   Установочная дискета Windows 2000 Server №4.
2. Вставьте компакт-диск Microsoft Windows 2000 Server в привод CD-ROM.
3. Если откроется диалоговое окно автозапуска компакт-диска Windows 2000, выберите пункт Exit (Выход).
4. Откройте окно командной строки.
5. В командной строке перейдите в корневой каталог компакт-диска, например, если привод CD-ROM обозначен буквой E, наберите E: и нажмите Enter.
6. В командной строке перейдите в каталог Bootdisk: наберите **cd bootdisk** и нажмите клавишу Enter,
7. Если Вы создаете загрузочные дискеты на компьютере с MS-DOS, 16-разрядной ОС семейства Windows или Windows 9x, наберите **makeboot a:** (где a: — имя дисковода для гибких дисков) и нажмите Enter. Если Вы создаете загрузочные дискеты на компьютере с Windows NT/2000, наберите **makebt32 a:** (где a: — имя дисковода для гибких дисков) и нажмите Enter.

   Windows 2000 попросит Вас подготовить 4 дискеты — в дальнейшем они будут использованы для установки Windows 2000.
8. Нажмите любую клавишу для продолжения.

   Windows 2000 предложит Вам вставить первую дискету.
9. Вставьте чистую отформатированную «Установочную дискету Windows 2000 Server № 1», и нажмите любую клавишу для продолжения.

   После копирования образа диска Вам будет предложено вставить следующую дискету. Создав таким образом 4 загрузочные дискеты Windows 2000, Вы увидите сообщение о завершении процесса.
10. В командной строке наберите **exit** и нажмите клавишу Enter.
11. Выньте дискету и компакт-диск.

► Задание 2: выполните предварительное копирование и перейдите в текстовый режим установки Windows 2000 Server

Этот этап выполняйте на Computer 1. Предполагается, что на нем не установлена никакая ОС, диск не разбит на разделы и отключена функция загрузки с компакт-диска. Для проверки соответствия Computer 1 всем требованиям см. раздел «Об этой книге».

1. Вставьте «Установочную дискету Windows 2000 Server №1», вставьте компакт-диск Windows 2000 Server в привод CD-ROM и перезагрузите компьютер.

   После перезагрузки программа Setup выдаст сообщение о проверке системной конфигурации, и откроется окно Windows 2000 Setup.

   Серый индикатор внизу экрана указывает, что компьютер исследуется и что загружается Windows 2000 Executive — сокращенная версия ядра Windows 2000.
2. В ответ на запрос вставьте вторую дискету и нажмите клавишу Enter.

   Setup сообщит о загрузке HAL, шрифтов, региональных параметров, драйверов шины и других программных компонентов для поддержки системной платы Вашего компьютера, шины и прочих аппаратных средств. Затем загружаются файлы, необходимые программе установки Windows 2000.
3. В ответ на запрос вставьте третью дискету и нажмите Enter.

Setup загрузит драйверы дисковых контроллеров и инициализирует их. В ходе этого процесса Setup может несколько раз приостанавливаться.

4. В ответ на запрос вставьте четвертую дискету и нажмите Enter.

   Будут выполнены загрузка драйверов поддержки периферийных устройств, например драйверов файловых систем, инициализация Windows 2000 Executive, и оставшаяся часть Setup.

   Если Вы устанавливаете пробную версию Windows 2000, откроется окно с соответствующим сообщением.

5. Прочитайте сообщение Setup и нажмите клавишу Enter.

   Заметьте: помимо новой установки Windows 2000, можно восстановить поврежденную установку Windows.

6. Прочитав приветственное сообщение, нажмите клавишу Enter.

   Setup выведет текст лицензионного соглашения.

7. Прочитав соглашение, нажмите клавишу F8, чтобы принять его условия.

   Вам будет предложено выбрать раздел для установки Windows 2000. Здесь же Вы сможете создать или удалить разделы на жестком диске.

   Если на жестком диске Computer ! нет разделов (как требуется для этого упражнения), Setup отобразит неразмеченную область.

8. Выделите в списке пункт Unpartitioned space (Неразмеченное пространство) и нажмите клавишу С.

   Setup попросит подтвердить намерение создать новый раздел и сообщает о его допустимом минимальном и максимальном размере.

9. Укажите размер нового раздела — 2048 Мб — и нажмите Enter.

Примечание Хотя в ходе установки разрешается создавать дополнительные разделы на остальном пространстве, рекомендуется разбивать диск на разделы после установки Windows 2000. Для этого применяется оснастка Disk Management (Управление дисками).

   Новый раздел будет отображен как C: New (Unformatted) [C; Новый (неформатированный)].

10. Выделите новый раздел и нажмите клавишу Enter.

    Вам будет предложено выбрать файловую систему для этого раздела.

11. Клавишами-стрелками выберите Format The Partition Using The NTFS File System (Форматировать раздел в системе NTFS) и нажмите Enter.

    Setup отформатирует раздел под NTFS и проверит жесткий диск на физические ошибки, которые могут помешать установке. Затем файлы Windows 2000 Server будут скопированы на жесткий диск компьютера. Этот процесс займет несколько минут, после чего компьютер будет перезагружен.

12. Выньте установочную дискету до перезагрузки.

Внимание! Если Ваш компьютер поддерживает загрузку с компакт-диска и эта функция не отключена в BIOS, загрузка будет выполнена с установочного компакт-диска Windows 2000 Server. Тогда Setup запустится повторно. Если это произошло, выньте компакт-диск и перезагрузите компьютер.

---

13. Setup скопирует дополнительные файлы, перезагрузит компьютер и вызовет мастер установки Windows.

► **Задание 3: продолжите установку в графическом режиме**

1. В окне приветствия мастера установки Windows 2000 щелкните кнопку Next (Далее) для сбора информации о компьютере.

   Setup сконфигурирует разрешения NTFS для системных папок и файлов, обнаружит аппаратные устройства, установит и сконфигурирует драйверы устройств для поддержки обнаруженной аппаратуры. Пропесс займет несколько минут.

2. В окне Regional Settings (Язык и стандарты) удостоверьтесь в правильной настройке региональных параметров системы и раскладки клавиатуры и щелкните Next.

   Setup отобразит окно Personalize Your Software (Настройка принадлежности программ), предлагая ввести Ваше имя и название Вашей организации. Эти сведения нужны для генерации стандартного имени компьютера. Многие приложения, которые Вы установите позже, будут использовать эту информацию для регистрации программы и идентификации документов.

Примечание Вы можете изменить региональные параметры и после установки — из окна Regional Options (Язык и стандарты), вызываемом из панели управления Windows.

---

3. В поле Name (Имя) введите свое имя, в поле Organization (Организация) — название организации и щелкните Next.

Примечание Если откроется окно Your Product Key (Ключ продукта), введите серийный номер Windows 2000 Server и щелкните Next.

   В окне Licensing Modes (Режимы лицензирования) Вам предлагается выбрать режим лицензирования и ввести число лицензий. По умолчанию выбран режим Per Server (На сервер).

4. Убедитесь, что в счетчике рядом с переключателем Per Server Number of concurrent connections (На сервер. Число одновременных подключений) указано 5, и щелкните Next.

Внимание! В данном курсе предполагается, что при установке выбран режим Per Server и разрешено 5 одновременных подключений к серверу. Вы должны указывать разрешенное количество подключений, основанное на имеющихся у Вас лицензиях. Вы можете также выбрать режим Per Seat вместо Per Server.

   Откроется окно Computer Name And Administrator Password (Имя компьютера и пароль администратора). Для генерации имени компьютера применяется введенное Вами название организации.

5. В поде Computer Name (Имя компьютера) введите **Server01**.

   Windows 2000 отображает имя компьютера прописными буквами независимо от того, как оно было введено.

Внимание! Чтобы завершить это упражнение, Ваш компьютер не должен быть подключен к сети.

   На практических занятиях Вы будете использовать компьютер Server01. Если Вы присвоили компьютеру другое имя, подставляйте его везде, где в тексте есть ссылка на ServerOl.

6. В полях Administrator Password (Пароль администратора) и Confirm Password (Подтверждение) введите **password** (строчными буквами) и щелкните кнопку Next (Далее). Пароли чувствительны к регистру букв, поэтому набирайте его только строчными буквами.

   Для выполнения упражнений данного учебного курса **Вы** будете вводить пароль учетной записи Administrator (Администратор). В реальных системах всегда следует использовать сложный пароль для этой учетной записи, содержащий буквы в верхнем и нижнем регистрах, цифры и символы, например Lp6*g9.

   Откроется окно Windows 2000 Components (Компоненты Windows 2000). Вы вправе установить дополнительные компоненты уже после установки ОС из окна Add/Remove Programs (Установка и удаление программ), которое открывается из панели управления Windows. На данном этапе устанавливайте только компоненты, выбранные по умолчанию. Дополнительные компоненты Вы установите позже в ходе обучения.
7. Щелкните Next.

   Если в ходе установки обнаружен модем, откроется окно Modem Dialing Information (Сведения о модеме).
8. Если открылось окно Modem Dialing Information (Сведения о модеме), введите телефонный код города и щелкните Next.

   Откроется окно Date and Time Settings (Настройка времени и даты).

Внимание! Службы Windows 2000 выполняют множество задач, успешное завершение которых зависит от настройки времени и даты. Выберите соответствующий часовой пояс во избежание проблем при выполнении упражнений.

---

9. Укажите дату, время и часовой пояс, а затем щелкните Next.

   Откроется окно Network Settings (Сетевые параметры), а затем будут установлены сетевые компоненты.

▶ Задание 4: завершите установку сетевых компонентов Windows 2000 Server

Средства работы в сети — неотъемлемая часть Windows 2000 Server. Параметров и конфигураций этих инструментов очень много. Здесь Вы сконфигурируете основные сетевые средства, а в одном из следующих упражнений установите дополнительные.

1. В окне Networking Settings (Сетевые параметры) выберите Typical Settings (Типичные параметры) и щелкните Next.

   При этом будут установлены сетевые компоненты для доступа и совместного использования сетевых ресурсов, а также сконфигурирован протокол **TCP/IP** для автоматического получения **IP-адреса** от сервера **DHCP.**

   В окне Workgroup Or Computer Domain (Рабочая группа или домен) предлагается присоединить Ваш компьютер к рабочей группе или домену.
2. Укажите, что Ваш компьютер не подключен к сети или подключен к сети без домена, что имя рабочей группы — WORKGROUP, и щелкните Next.

   В окне Installing Components (Установка компонентов) отображается ход установки и конфигурирования выбранных компонентов ОС. Это займет несколько минут.

   Откроется окно Performing Final Tasks (Выполнение заключительных действий), отображающее ход выполнения оставшихся задач: копирования файлов, создания и сохранения изменений конфигурации и удаления временных файлов. Маломощным компьютерам для этого может потребоваться более получаса.

   Затем откроется окно Completing the Windows 2000 Setup Wizard (Завершение установки Windows 2000).

3. Выньте компакт-диск Windows 2000 Server из привода CD-ROM и щелкните кнопку Finish (Готово).

Внимание! Если Ваш компьютер поддерживает загрузку с компакт-диска и Вы не удалите установочный компакт-диск, установка будет повторно инициирована после перезагрузки компьютера. Если это произошло, выньте компакт-диск и перезапустите компьютер.

После перезагрузки будет запущена установленная версия Windows 2000 Server.

► Задание 5: завершите установку аппаратных средств

На заключительной стадии устанавливаются все устройства Plug and Play, не обнаруженные на предыдущих этапах установки.

1. Нажмите клавиши Ctrl + Alt+Delete.
2. В диалоговом окне регистрации в системе в поле User Name (Пользователь) введите **Administrator** (Администратор), а в поле Password (Пароль) — **password**.
3. Щелкните OK.

   Если Windows 2000 обнаружит новые аппаратные средства, откроется окно мастера Found New Hardware (Мастер обнаружения нового оборудования), сообщающее об установке соответствующих драйверов.
4. Если открылось окно мастера, укажите, что перегружать компьютер после установки устройств не нужно и щелкните кнопку Finish (Готово), чтобы завершить работу мастера.

   Откроется диалоговое окно Configure Your Server (Настройка сервера Windows 2000), откуда Вы можете сконфигурировать ряд дополнительных параметров и функций.
5. Щелкните переключатель I Will Configure This Server Later (Я выполню настройку этого сервера позже), а затем — кнопку Next.
6. В следующем окне сбросьте флажок Show This Screen At Startup (Открывать это окно при загрузке).
7. Закройте окно Configure Your Server.

► Задание 6: настройте параметры экрана

Setup выбирает стандартное разрешение, совместимое с обнаруженной видеоплатой. Вы можете изменить стандартные параметры сейчас или после установки Windows 2000.

Внимание! Если Вы не знаете частоту обновления, поддерживаемую Вашим монитором с выбранной Вами цветовой палитрой и размером экранной области, не меняйте параметры по умолчанию. Завышенное значение частоты обновления может повредить монитор.

---

1. Если Вы хотите скорректировать параметры экрана (увеличить количество цветов или разрешение), откройте панель управления и дважды щелкните значок Display (Экран).

   Откроется диалоговое окно Display Properties (Свойства: Экран).
2. Перейдите на вкладку Settings (Настройка), измените область экрана и цветовую палитру, а затем щелкните кнопку OK.

   Окно Display Properties (Свойства: Экран) предупредит Вас о временном применении новых параметров.
3. Щелкните кнопку OK.

   Если выбранные Вами параметры верны, откроется окно сообщения Monitor Settings (Параметры монитора).

4. Щелкните кнопку Yes (Да), чтобы изменения вступили в силу окончательно.
5. Закройте панель управления.

Примечание Для корректного завершения работы Windows NT Server в меню Start (Пуск) выберите команду Shut down (Завершение работы).

Резюме

Для установки Windows 2000 Server служит программа Winnt.exe или Winnt32.exe. Первая применяется на компьютерах с MS-DOS или 16-разрядными версиями Windows, вторая — на компьютерах с 32-разрядными версиями Windows (Windows 9x/NT/2000). Для настройки способа установки вместе с этими программами можно использовать ряд ключей. Процесс установки состоит из 3 этапов: предварительного копирования, текстового и графического режима. Сначала нужные для установки файлы копируются *во* временные каталоги на локальном жестком диске. В текстовом режиме Setup позволяет создать или удалить разделы на жестком диске, куда затем будет установлена ОС. В графическом режиме Вы можете выбрать необязательные компоненты и указать пароль администратора.

Занятие 3. Обновление до Windows 2000 Server

Процесс обновления серверов Windows NT до Windows 2000 Server автоматизирован. В ходе обновления Setup перемешает текущие параметры ОС, практически не требуя участия администратора. Мы обсудим три аспекта обновления: обновление до Windows 2000 Server, обновление доменов Windows NT и консолидацию доменов.

Изучив материалы этого занятия, Вы сможете:

- ✓ обновить Windows NT до Windows 2000 Server.

Продолжительность занятия — около 30 минут.

Обновление до Windows 2000 Server

В начале установки запускается мастер, который проведет Вас через все этапы обновления. В окне выберите Upgrade To Windows 2000 (Обновление до Windows 2000). На заключительных стадиях установки мастер соберет сведения об особенностях настройки предыдущей ОС.

Есть несколько причин предпочесть обновление, если предыдущая ОС это допускает: упрощается конфигурация, сохраняются существующие учетные записи, параметры настройки, группы и разрешения, не надо переустанавливать приложения и восстанавливать файлы данных. Впрочем, как и при любых серьезных изменениях системы, перед запуском Setup обязательно создайте резервную копию жесткого диска.

Если Вы хотите обновить ОС и использовать ранее установленные программы, изучите руководство по совместимости приложений с Windows 2000 по адресу *http://www.microsoft.com,* а также прочитайте файлы Readlst.txt и Retnotes.doc (в корневом каталоге установочного компакт-диска). Вы можете установить средства поддержки Windows 2000, расположенные в каталоге \Support\Tools установочного компакт-диска.

При обновлении ОС Вы должны решить, следует ли преобразовать файловую систему на имеющихся разделах FAT16 или FAT32 в NTFS. Разрешается установить Windows 2000 Server совместно с другой ОС, хотя применение двухвариантной загрузки может усложнить работу с системой, а потому не рекомендуется.

Обновление серверов

Windows 2000 Server поддерживает обновление Windows NT 3.51/4.0 и предыдущих версий Windows 2000 Server. Если на компьютере установлена Windows NT до версии 3.51, сначала обновите ее до версии 4.0 и лишь затем — до Windows 2000 Server.

Примечание Windows 2000 поддерживает все пакеты исправлений для Windows NT 3.51/4.0. Обновление установленных приложений к обновлению ОС отношения не имеет и проводится отдельно.

Способы обновления

Проще всего обновить Windows NT Server так: вставить установочный компакт-диск Windows 2000 Server и запустить Winnt32.exe.

Setup не позволяет обновить ОС при загрузке с дискет или компакт-диска — для этого используется Winnt32.exe. Обновление также можно выполнить, запустив Winnt32.exe с другого компьютера в сети.

Поиск предыдущих установок Windows NT

Для поиска предыдущих версий Windows NT Server на системах с процессорами x86 исследуется файл C:\Boot.ini.

Примечание Windows 2000 не поддерживает системы с RISC-процессорами.

Setup пытается обратиться к файлу *<активный_раздел>*:\Boot.ini. Активный раздел, как правило, C:. Корневой каталог этого диска просматривается в поисках:

- каталогов — Setup ищет каталоги System32, System32\Drivers и System32\Config;
- файлов — в подкаталогах System32 идет поиск файлов Ntoskrnl.exe и Ntdll.dll.

Затем Setup пытается загрузить фрагменты системного реестра, чтобы определить, предпринимались ли ранее попытки обновить ОС и насколько они были успешны. Также определяется тип текущей установки Windows NT, ее вариант (Server или Workstation), номер версии Windows (3.1, 3.5, 3.51 или 4.0) и номер выпуска.

Текущая версия системы и номер выпуска должны быть меньше или равны номеру версии ОС, до которой Вы хотите обновить систему. Редакция должна быть Server. Так что разрешается обновить до Windows 2000 Server только Windows NT Server 3.51 и 4.0.

В результате этого анализа выводится список предыдущих ОС, допускающих обновление. Если установка Windows NT Server не появляется в этом списке, она, вероятно, не соответствует одному из упомянутых условий. Тогда, нажав F3, можно отказаться от обновления и продолжить использовать имеющуюся версию Windows NT.

Примечание Если в файле C:\Boot.ini несколько записей указывают на одну установку Windows, она упоминается в списке выбора обновления только раз.

Обновление домена Windows NT

Это важнейшая задача при обновлении до Windows 2000 Server. Домен объединяет учетные записи и сетевые ресурсы под одним доменным именем в рамках единой политики защиты.

В Windows 2000 серверы могут выполнять одну из трех ролей:

- контроллер домена — хранит учетные записи и другие данные Active Directory для этого домена;
- член домена — рядовой сервер, принадлежит домену, но не хранит данные Active Directory;
- изолированный сервер — относится не к домену, а к рабочей группе.

В домене должен быть минимум один контроллер, хотя рекомендуется создать несколько контроллеров, каждый из которых будет хранить резервные копии учетных записей и данных Active Directory и обеспечивать регистрацию пользователей в системе.

Вы должны заранее решить, что будут делать Ваши серверы, хотя роль сервера разрешено изменить и после установки. Несколько важных аспектов следует учесть при обновлении существующего домена Windows NT:

- на контроллерах домена надо использовать файловую систему NTFS;
- Вы не сможете обеспечить эффективную защиту сервера, установленного на разделах с FAT16 или FAT32: на таких разделах доступ к общим папкам регулируется разрешениями на уровне каталогов, но не отдельных файлов; локальный доступ к этим разделам вообще не ограничен;
- сначала должен быть обновлен основной контроллер домена Windows NT,

Кроме того, если в Windows NT Server существовали *основные* (primary domain controller, PDC) и *резервные* (backup domain controller, BDC) *контроллеры домена,* то в Windows 2000 все контроллеры равноправны. Таблица поможет Вам понять, как программа установки Windows 2000 назначает роли сервера при обновлении:

Роль в домене Windows NT	Роль в домене Windows 2000
Основной контроллер домена	Контроллер домена
Резервный контроллер домена	Контроллера домена или рядовой сервер домена на Ваш выбор
Рядовой сервер	Рядовой или изолированный сервер на Ваш выбор
Изолированный сервер	Рядовой сервер (если есть домен Windows 2000) или изолированный сервер на Ваш выбор

Обновление домена Windows NT включает несколько стадий:

- планирование обновления домена Windows NT;
- подготовка к обновлению домена Windows NT;
- обновление основного контроллера домена;
- обновление резервных контроллеров домена;
- обновление рядовых серверов домена.

Планирование обновления домена Windows NT

- **Организация доменных имен DNS.** Разработайте структуру DNS для корневого домена дерева или нескольких деревьев, объединенных в лес отдельных доменных DNS. Создав корневой домен DNS, в его дерево можно добавить дочерние домены. Например, если microsoft.com — корневой домен, то домены dev.microsoft.com и mktg.microsoft.com будут его дочерними доменами.
- **Организация пространства имен в доменах с большим количеством учетных записей.** Решите, как структурировать ресурсы Вашего предприятия, разбив сеть на организационные подразделения (ОП).
- **Консолидация домена.** Централизуйте администрирование сетевых служб, объединив домены ресурсов в меньшее число доменов Windows 2000.
- **Учетные записи компьютеров.** Распределите учетные записи компьютеров по ОП. Это важная часть внедрения политики защиты.
- **Внедрение новых технологий. Не** забывайте о новых технологиях, например, используйте инфраструктуру секретных ключей для регистрации пользователей по смарт-картам и аутентификации удаленного доступа.

Примечание **См.** также руководство «Windows 2000 Support Tools' Deployment and Planning Guide». Программа установки этого руководства и других средств поддержки находится в каталоге \support\tools на компакт-диске Windows 2000 Server.

Подготовка к обновлению домена Windows NT

Перед серьезными изменениями содержимого жестких дисков сделайте их копии. Кроме того, перед обновлением основного контроллера домена отсоедините от локальной сети кабель резервного контроллера, После обновления основного контроллера до Windows 2000 Server резервный контроллер можно сделать основным.

Убедитесь также, что на будущем контроллере домена Windows 2000 хватает свободного места на диске сверх необходимого самой ОС. В результате обновления база данных (БД) учетных записей пользователей может заметно увеличиться.

Подготовка к обновлению контроллера домена

Чтобы преобразовать БД WINS, отключите WINS в окне Services, которое открывается из панели управления Windows NT Server 4.0. Чтобы преобразовать БД DHCP, в том же окне отключите сервер DHCP. Создайте тестовые учетные записи, чтобы проверить эффективность обновления.

Ниже описаны элементы, которые можно включить в тестовую среду.

Элемент	Выполнение
Политика пользователей и групп	Включает пользовательскую и групповую политику, действие которых можно легко проверить после обновления. Для примера удалите из меню Start (Пуск) на компьютерах пользователей команду Run (Выполнить).
Профили пользователя	Настройте простые индивидуальные профили для тестовых пользователей, например меняющие фоновый рисунок рабочего стола.
Сценарии входа в систему	Разработайте простой в проверке сценарий входа, например подключающий сетевые диски командой net use.

Примечание Рекомендуется всегда первоначально проверять любое серьезное обновление в лабораторной среде. Для этого можно удалить из сети резервный контроллер и повысить его уровень до основного контроллера в отдельной тестовой сети. Затем обновите оставшийся в сети основной контроллер до Windows 2000 Server. Если все пройдет успешно, Вы сможете вернуть этот компьютер в реальную сеть.

Обновление основного контроллера домена

Процедура обновления всегда должна сначала выполняться над главным контроллером домена. При этом Вам будет предложен выбор; создать новый или дочерний домен или создать новый лес или дерево доменов в существующем лесу. Для обновления домена, состоящего из 3–5 серверов, создайте новый домен и новый лес. Определите и пространство имен домена, чтобы настроить пространство имен верхнего уровня для Вашей организации. Другие домены могут быть добавлены в его дерево как дочерние.

В ходе обновления Вы вправе выбрать место хранения трех важных файлов: БД, содержащей учетные записи.и другие данные Active Directory, журнала и файла системного тома (SYSVOL). БД и журнал разрешается хранить на разделе любого типа (FAT16, FAT32 или NTFS). Учтите: предыдущая БД в результате обновления может заметно увеличиться. Журнал, напротив, изначально будет невелик. Файл системного тома должен храниться на разделе с NTFS.

Обновленный контроллер домена будет полностью совместим с остальными серверами Вашей сети. Это значит, что серверами и клиентами Windows 2000 новый контроллер домена будет восприниматься как полноценный контроллер домена Windows 2000, а для других серверов и клиентов он будет эмулировать основной контроллер Windows NT 4.0.

Обновление резервного контроллера домена

После успешного обновления основного контроллера можно приступить к обновлению резервных. Для этого первый обновленный сервер (бывший основной контроллер) должен быть доступен в сети. Этот сервер используется как шаблон для обновления остальных контроллеров домена.

Обновляйте резервные контроллеры по очереди, каждый раз предварительно создавая их резервные копии. Перед преобразованием следующего резервного контроллера обязательно проверьте в сети работоспособность только что обновленного.

После обновления всех серверов до контроллеров домена Windows 2000 разрешается перевести домен из *смешанного* (Mixed) режима, предусматривающего существование в домене контроллеров Windows NT, в *основной* (Native), когда в домене допускаются только контроллеры Windows 2000.

Внимание! Обратный переход из смешанного режима в основной невозможен.

Рис. 2-2 иллюстрирует процесс трансформации домена Windows NT в домен Windows 2000 основного режима.

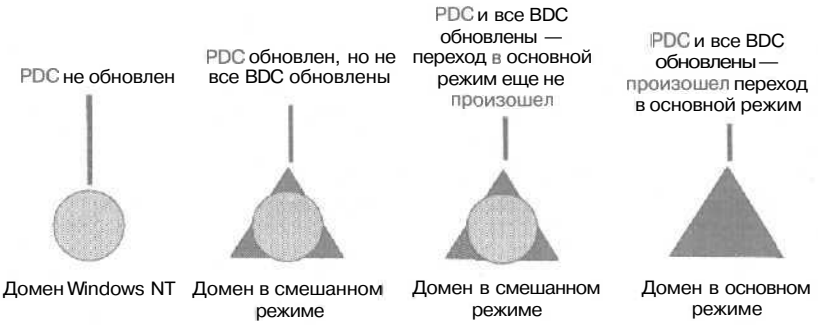


Рис. 2-2. **Переход от домена Windows NT к домену Windows 2000 основного режима**

Смешанный режим

Характеризует домен, одновременно содержащий контроллеры Windows 2000 и Windows NT 3.51/4.0. В смешанном режиме основной контроллер обновляется до Windows 2000 Server, а на резервных контроллерах остается Windows NT Server 3.51/4.0. Контроллер домена Windows 2000, бывший главный контроллер, использует для описания объектов хранилище Active Directory. Он все еще полностью совместим с контроллерами предыдущих версий Windows и предоставляет данные подчиненным компьютерам в плоском хранилище.

Для компьютеров с Windows 2000 обновленный PDC отображается как контроллер домена Windows 2000, а для остальных — как контроллер домена Windows NT 3.51/4.0. В домене по-прежнему применяется схема репликации с одним хозяином — новым PDC Windows 2000.

В смешанном режиме домен ограничен функциональными возможностями контроллера домена Windows NT 4.0. Вот некоторые из этих ограничений:

- запрещена вложенность групп;
- клиенты с предыдущими версиями Windows не могут извлечь выгоду из транзитивных доверительных отношений; доступ к ресурсам осуществляется, как в доменах предыдущих версий Windows.

Смешанный режим применяется по умолчанию и является промежуточным этапом в процессе внедрения Windows 2000.

Основной режим

После обновления всех контроллеров домена его можно перевести в основной режим, в котором все клиенты используют транзитивные доверительные отношения Windows 2000, т. е. способны соединиться с любым ресурсом предприятия. В основном режиме допускается вложенность групп.

Внимание! Переход в основной режим является односторонним — вернуться к смешанному затем нельзя.

Обновление рядовых серверов

Рядовые серверы домена разрешается обновлять в произвольном порядке.

Консолидация домена

Подразумевает реорганизацию ресурсов домена в целях использования новых расширенных возможностей Active Directory. Переконфигурировать домен для развертывания Windows 2000 не надо — это можно сделать после обновления остальных компьютеров и включения их в домены. Реконфигурация — дело трудоемкое, и понимается под ней перемещение компьютеров в новые домены, а также проверка и корректировка их параметров доступа.

Объединить домены можно двумя основными способами:

- переместить учетные записи из одного домена в другой для формирования одного большого домена;
- переместить серверы из одного домена ресурсов в ОП другого домена.

Преимущество консолидации — в сокращении числа доменов, регистрирующих пользователей, так как в Windows 2000 каждый домен может хранить сведения о гораздо большем количестве пользователей, групп и учетных записей. Объединение позволяет также сократить число междоменных доверительных отношений. Впрочем, при перемещении учетных записей пользователей потребуется создать для них временные пароли в новом домене, поскольку пользовательские пароли при переносе не сохраняются — только *идентификатор безопасности* (security identifier, SID).

Еще один плюс консолидации — возможность уменьшить количество доменов ресурсов, переместив серверы из маленьких доменов в объединенный. Контроллеры доменов ресурсов станут серверами — членами консолидированного домена. Это позволит сократить число междоменных доверительных отношений между доменами ресурсов и контроллерами доменов и сэкономить системные ресурсы последних. Консолидация также упрощает перевод серверов из одного проекта или отдела в другой.

Windows 2000 включает следующие возможности реконфигурации домена.

- При пересечении пользователями и группами границ домена их атрибуты защиты сохраняются. Хронология SID хранится с учетной записью, и маркеры доступа будут содержать и новый и старый SID, чтобы сохранить права доступа.
- Контроллеры домена разрешается понижать до уровня рядового сервера и перемещать в другой домен.
- Политику защиты можно централизованно применять ко многим системам. Новый компьютер при присоединении к домену автоматически принимает его политику защиты.

- Допускается перемешать компьютеры между доменами средствами удаленного администрирования.
- Для отражения изменений в структуре организации или способе ее представления можно соответственно модифицировать права доступа.

Резюме

Обновление Windows NT Server до Windows 2000 Server в значительной мере автоматизировано. Простейший способ обновить Windows NT Server — вставить установочный компакт-диск Windows 2000 Server в привод CD-ROM и запустить программу Winnt32.exe; остальное поможет сделать мастер. Для успешного обновления надо разработать структуру доменных имен и выполнить ряд подготовительных операций, включая резервное копирование и разъединение сетевых кабелей. Вы также должны подготовиться к обновлению контроллеров домена. Сначала надо обновить главный контроллер, затем резервные контроллеры и рядовые серверы домена. По завершении обновления серверов надо решить, консолидировать ли домен, чтобы задействовать преимущества Active Directory.

Занятие 4. Устранение неполадок при установке Windows 2000 Server

Мы рассмотрим некоторые типичные проблемы, с которыми Вы можете столкнуться в ходе установки.

Изучив материалы этого занятия, Вы сможете:

- ✓ устранить неполадки при установке Windows 2000.

Продолжительность занятия — около 15 минут.

Устранение неполадок при установке Windows 2000 Server

Вы можете столкнуться с проблемами, вызванными, например, испорченными носителями или несовместимыми аппаратными средствами.

Проблема	Решение
Ошибки носителей	Если Вы устанавливаете ОС с компакт-диска, попробуйте использовать другой привод CD-ROM. Если ошибки повторятся, замените установочный компакт-диск, связавшись с Microsoft или Вашим поставщиком ОС.
Неподдерживаемое устройство чтения компакт-дисков	Замените привод CD-ROM на совместимый. Если это невозможно, попробуйте установить ОС иначе, например по сети. По завершении установки Вы сможете установить соответствующий драйвер для Вашего привода CD-ROM.
Не хватает места на диске	С помощью Setup создайте достаточно большой раздел или переформатируйте существующий, увеличив его объем.
Проблемы сетевой идентификации	Вернитесь в диалоговое окно Network Settings мастера установки Windows 2000 и проверьте, что Вы выбрали правильный протокол и сетевую плату. Проверьте конфигурацию сетевой платы, например тип трансивера, и уникальность имени компьютера в сети.
Невозможно соединиться с контроллером домена	Проверьте правильность имени домена. Убедитесь, что на сервере запущена служба DNS и что сервер и контроллер доступны в сети. Если найти контроллер домена нельзя, создайте рабочую группу и присоединитесь к домену после установки. Проверьте параметры сетевой платы и протокола. Если Вы переустанавливаете Windows 2000, используя то же самое имя компьютера, удалите и повторно создайте его учетную запись.
Ошибка при установке или запуске Windows 2000 Server	Убедитесь, что Windows 2000 обнаружила все аппаратные средства и что они перечислены в HCL.

Резюме

Проблемы установки зачастую вызваны испорченными носителями или несовместимыми аппаратными средствами. Кроме того, на выбранном Вами разделе может не хватать места для установки Windows 2000 Server, Иногда из-за неверных параметров сети сервер неспособен соединиться с контроллером домена, что также помешает завершить установку.

Закрепление материала

? J Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Какую файловую систему выбрать при установке Windows 2000 для двухвариантной загрузки? Почему?

2. Пользователям в Вашей организации зачастую нужен доступ к нескольким серверам. Какой режим лицензирования следует выбрать и почему?

3. Вы устанавливаете Windows 2000 Server на компьютере, который будет рядовым сервером в имеющемся домене Windows 2000. В ходе установки Вы хотите присоединить компьютер к домену. Какая информация Вам нужна и какие компьютеры должны быть доступны в сети перед запуском программы установки?

4. Вы устанавливаете Windows 2000 Server с компакт-диска на компьютере, который ранее работал под управлением другой ОС. На жестком диске не хватает места для обеих ОС, и Вы решили заново поделить жесткий диск на разделы и установить Windows 2000 Server на чистый жесткий диск. Опишите два способа деления жесткого диска на разделы.

5. Вы устанавливаете Windows 2000 по сети. Какие операции необходимо выполнить на клиентском компьютере перед установкой?

6. Вы хотите обновить Windows NT 3,5 Server до Windows 2000. Выберите из списка все возможные способы обновления;
   а) выполнить обновление до Windows NT 3.51 Workstation и затем — до Windows 2000 Server;
   б) выполнить обновление до Windows NT 4.0 Server и затем — до Windows 2000 Server;
   в) сразу выполнить обновление до Windows 2000 Server;
   г) запустить программу Convert.exe, чтобы обеспечить совместимость имеющихся разделов NTFS с Windows 2000, и выполнить обновление до Windows 2000 Server;
   д) выполнить обновление до Windows NT 3.51 Server и затем — до Windows 2000 Server.

7. В Вашей сети ощущается нехватка дискового пространства. Опишите три службы в Windows 2000 Server, которые помогут контролировать и эффективно использовать имеющееся пространство.

ГЛАВА 3

Автоматическая установка Windows 2000 Server

В этой главе

Установку Windows 2000 Server и серверных приложений на несколько компьютеров можно автоматизировать, создав файл ответов (сценарий, автоматически отвечающий на запросы программы установки) и запустив Setup из командной строки с соответствующим параметром.

Прежде всего

Для изучения материалов этой главы потребуется:

- установить Windows 2000 Server на Server01, как указано в упражнении 1 главы 2;
- подключить Computer 2 по сети к ServerOl и установить на нем 32-разрядную версию Windows;
- убедиться, что Computer 2 отвечает минимальным аппаратным требованиям, описанным в разделе «Об этой книге»;
- установочный компакт-диск Windows 2000 Server.

Занятие 1. Подготовка к автоматической установке Windows 2000 Server

Перед автоматической установкой Windows 2000 Server надо создать файл ответов, предоставляющий информацию для Setup. Для установки Windows 2000 Server на нескольких компьютерах по сети требуется минимум один набор дистрибутивных папок. Здесь рассказано о создании файла ответов и определении дистрибутивных файлов для сетевой установки.

Изучив материалы этого занятия, Вы сможете:

- ✓ создать файл ответов;
- ✓ установить дистрибутивный каталог для сетевой установки Windows 2000.

Продолжительность занятия — около 45 минут.

Создание файла ответов

Файл ответов (обычно с расширением .txt) является специализированным сценарием, позволяющим выполнить автоматическую установку Windows 2000 Server. Этот файл, иногда называемый *сценарием автоматической установки,* отвечает на вопросы, которые Setup задает пользователю при обычной установке. Каталог \i386 установочного компакт-диска Windows 2000 Server содержит примеры таких файлов. Имя файла ответов можно изменить в соответствии с потребностями организации. Так, Compl.txt, Install.txt и Setup.txt — правильные имена файлов ответов, если они верно указаны в команде установки. Сценарии с разными именами можно настроить для разных установок на разных типах компьютеров.

Заметьте: другие программы, скажем, утилита Sysprep, для создания образа диска установки Windows 2000 Server тоже используют файлы ответов, (Подробнее о Sysprep см. занятие 2.) Вот возможные имена файлов ответов в зависимости от их использования:

Имя файла	Когда используется
<имя_файла>.txt	При автоматической установке. Можно указать любое имя файла. Unattend.txt — имя файла ответов, поставляемого с Windows 2000 Server.
Winnt.sif	При установке Windows 2000 Server с загрузочного компакт-диска.
Sysprep.inf	При использовании утилиты Sysprep для создания образа установки Windows 2000 Server.

У файлов из этой таблицы тот же формат, что и в Unattend.txt. Файл ответов состоит из множества необязательных разделов, которые можно изменить согласно требованиям к установке. Он дает программе Setup ответы на все вопросы ручной установки Windows 2000 Server. Файл ответов также указывает Setup, как взаимодействовать с созданными вами установочными файлами и папками, Например, раздел [Unattended] содержит запись *изготовителя оборудования* (OEM), указывающую на необходимость копирования подпапки OEM из дистрибутивной папки на целевой компьютер.

Формат файла ответов

Файл ответов состоит из заголовков разделов, параметров и их значений. Большинство разделов уже определено, но некоторые из них переопределяются пользователем. Ниже

приведен листинг файла Unattend.txt. Его можно скопировать с компакт-диска на жесткий диск, отредактировать и переименовать.

```
;Microsoft Windows 2000 Professional, Server
;Advanced Server and Datacenter
; (c)1994 -1999 Microsoft Corporation. All rights reserved.
;
;Пример файла ответов для автоматической установки
;
;Этот файл содержит сведения о проведении автоматической
;установки или обновления
;Windows 2000 Professional и Windows 2000 Server.
;В результате Setup выполняется без запросов ввода от
;пользователя.
;
[Unattended]
Unattendmode - FullUnattended
OemPreinstall = NO
TargetPath = WINNT
Filesystem = LeaveAlone

[UserData]
FullName - "Ваше имя пользователя"
OrgName = "название Вашей организации"
ComputerName = "ИМЯ_КОМПЬЮТЕРА"

[GuiUnattended]
;Задает временную зону - Pacific Northwest
;Пароль администратора не задается (NULL)
;Включает автоматический однократный вход в систему
TimeZone - "004"
AdminPassword = *
AutoLogon - Yes
AutoLogonCount - 1

;Параметрылицензирования
[LicenseFilePrintData]
AutoMode - "PerServer"
AutoUsers = "5"

[GuiRunOnce]
;Перечислите здесь программы,
;которые надо запустить после первой процедуры регистрации

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
```

```
VRefresh = 70

[Networking]
;Если параметр InstallDefaultComponents равен YES,
;Setup устанавливает стандартные сетевые компоненты, включая
;протокол TCP/IP, службу доступа к файлам и принтерам
;и клиента для сетей Microsoft.
InstallDefaultComponents = YES

[Identification]
JoinWorkgroup - Workgroup
```

Файл автоматической установки разбит на разделы, имена которых заключаются в квадратные скобки, например:

```
[UserData]
```

В рамках разделов параметрам присваиваются соответствующие значения. Параметры и их значения отделяются друг от друга равным количеством пробелов:

```
BitsPerPel = 8
```

Значения с пробелами внутри заключаются в кавычки:

```
OrgName - "Microsoft Corporation"
```

Некоторые разделы не имеют параметров и просто содержат список значений:

```
[OEMBootFiles]
Txtsetup.oem
```

Строки примечаний начинаются с точки с запятой;

```
;В результате Setup выполняется без запросов ввода от пользователя.
```

Параметры и значения

Каждый параметр файла ответов должен иметь присвоенное ему значение; впрочем, некоторые параметры необязательны или отсутствуют, поэтому применяются значения по умолчанию. Значения параметров — обычно текстовые строки. Когда указано число, значение — десятичное (если явно не указана другая система счисления).

Примечание Имена параметров нечувствительны к регистру букв.

Подробные сведения о параметрах (и их значениях) файлов ответов см. в файле Unattend.doc. Он находится в архиве Deploy.cab на компакт-диске Windows 2000 Server в папке \Support\Tools. Для распаковки или просмотра содержимого архива Deploy.cab вызовите проводник Windows. Дополнительные сведения об открытии файла Unattend.doc см. в файле Sreadme.doc на установочном компакт-диске Windows 2000 Server.

Внимание! Запуск Setup.exe или 2000rkst.msi из папки \Support\Tools установит из архива Support.cab инструменты поддержки Windows 2000, однако Unattend.doc и прочие файлы из архива Deploy.cab не распаковываются.

Методы создания файла ответов

Создать файл ответов позволяют утилита Setup Manager (Диспетчер установки) из архива Deploy.cab или любой текстовый редактор.

Создание файла ответов с помощью Setup Manager

Setup Manager применяется для:

- указания базового продукта: Windows 2000, службы удаленной установки ОС или Sysprep;
- определения уровня автоматизации: Provide Defaults (Предоставление значений параметров по умолчанию), Fully Automated (Полностью автоматическая установка), Hide Pages (Не отображать диалоговые окна), Read Only (Только чтение) и GUI mode attended Setup (Полное взаимодействие с пользователем);
- задания информации по умолчанию для имен пользователя и организации;
- назначения одного или нескольких имен компьютеров (при множественных автоматических установках);
- определения до 99 автоматических входов в систему с полномочиями администратора с целью завершения процесса установки;
- настройки параметров экрана;
- настройки параметров сети;
- задания членства компьютера в рабочей группе или в домене с автоматическим добавлением в домен учетной записи компьютера;
- создания дистрибутивных папок;
- добавления файлов логотипа и фонового рисунка;
- добавления файлов в дистрибутивные папки;
- добавления команд в раздел [GuiRunOnce] файла автоматической установки;
- создания файла Cmdlines.txt;
- назначения кодовой страницы и других языковых параметров;
- указания региональных параметров;
- определения часового пояса;
- задания информации TAPI;
- настройки параметров обозревателя Web и оболочки;
- задания имени дистрибутивной папки; загрузочный раздел (содержащий файлы ОС) задается ключами /t: или /tempdrive:;
- добавления принтеров;
- добавления устройств накопителей и специализированных уровней **HAL,** используемых при автоматической установке;
- создания дистрибутивных папок с предоставлением к ним доступа для установки или назначения автоматической установки с компакт-диска Windows 2000 Server.

Setup Manager (Диспетчер установки) позволяет создать согласованный файл ответов. Впрочем, он не может задавать все параметры файла ответов или необязательные компоненты, создавать файлы Txtsetup.oem или подпапки в дистрибутивной папке,

Создав с помощью Setup Manager файл ответов, Вы можете добавить дополнительные параметры в текстовом редакторе. Полный список доступных параметров см. в файлах Unattend.doc и Readme.txt в архиве Deploy.cab.

Вот наиболее часто используемые параметры Setup Manager:

Параметр	Цель использования
Upgrade option (Платформа)	Указывает, что устанавливать: Windows 2000 Professional или Windows 2000 Server.
Target computer name (Имя компьютера)	Задает имена пользователя, организации и компьютера для установки на целевых компьютерах.
Product ID (Идентификационный номер продукта)	Задает номер лицензии продукта, содержащийся в его документации.
Workgroup or domain (Рабочая группа или домен)	Назначает имя рабочей группы или домена, в который будет добавлен компьютер.
Time zone (Часовой пояс)	Задает часовой пояс для компьютера.
Network configuration information (Сетевые параметры)	Задает тип сетевой платы и ее параметры, включая сетевые протоколы.

Создание файла ответов вручную

Для создания файла ответов вручную применяют текстовый редактор, например Notepad (Блокнот). Файл ответов состоит из раздела заголовков, параметров и их значений. Хотя большинство заголовков раздела уже определено, можно задать дополнительные. Кстати, в файле ответов не обязательно указывать все ответы.

В приложении Б приведены примеры файлов ответов, которые подходят для стандартной конфигурации. Вы можете настроить готовый файл ответов Unattend.txt, поставляемый с Windows 2000, или создать новый на основе приведенного примера.

Создание дистрибутивных папок

Для установки Windows 2000 Server на нескольких компьютерах по сети надо создать хотя бы один набор дистрибутивных папок, обычно располагающихся на сервере, к которому подключаются целевые компьютеры. Для установки Windows 2000 Server пользователи запускают на них программу Winnt.exe или Winnt32.exe. Для выполнения разных вариантов установки системы применяют один набор дистрибутивных папок и несколько файлов ответов. Даже если используется образ диска, папки установки помогут независимо установить разные типы систем. Дистрибутивные папки также позволяют изменять образы дисков, редактируя в них файлы, чтобы создавать индивидуальные образы, не начиная с самого начала.

Чтобы сбалансировать нагрузку на серверы и ускорить копирование установочных файлов Windows 2000 Server, можно создать дистрибутивные папки на нескольких серверах с учетом будущей установки на компьютерах с Windows 95-, Windows 98-, Windows NT- или Windows 2000. Winnt32.exe можно запустить с 8 наборами загрузочных папок, каждый из которых должен хранить дистрибутивные файлы Windows 2000 Server, драйверы устройств и другие файлы.

Для ручного создания дистрибутивной папки подключитесь к сетевому серверу, на котором Вы хотите ее разместить, и создайте папку \W2kdist на общедоступном сетевом ресурсе. Чтобы различать продукты семейства Windows 2000 (Professional, Server и Advanced Server), задайте каждой папке соответствующее имя. Если организация контактирует с зарубежными странами, при использовании локализованных версий Windows 2000 для каждой нужно создать отдельный дистрибутивный сетевой ресурс и скопировать в него содержимое папки \i386. Например, готовясь установить Windows 2000 Server, создайте папку \W2kdist, укажите к ней доступ и скопируйте туда каталог \i386 с установочного компакт-диска Windows 2000 Server.

Примечание Для дистрибутивного сетевого ресурса, с которого будет устанавливаться Windows 2000 Server по умолчанию, требуется около 313 Мб на диске.

Создать и открыть доступ к дистрибутивной папке позволяет также Setup Manager.

Структура дистрибутивной папки

Здесь подробно описаны папки и подпапки дистрибутивной папки (рис. 3-1).

\i386

Это главная дистрибутивная папка, включает все требуемые для установки Windows 2000 Server файлы. Ее содержимое копируют с установочного компакт-диска Windows 2000 Server в корневой каталог дистрибутивного сетевого ресурса.

\OEM

Копируется в WIN_NT.~LS с дистрибутивного сетевого ресурса. Подпапка \$OEM$ располагается уровнем ниже главной дистрибутивной папки. В процессе установки в \$OEMS автоматически копируются каталоги и файлы с именами формата 8.3 и инструменты, необходимые для автоматической установки. Задав в файле ответов параметр OEMFILESPATH, подпапку \$OEM$ можно создать вне дистрибутивной папки.

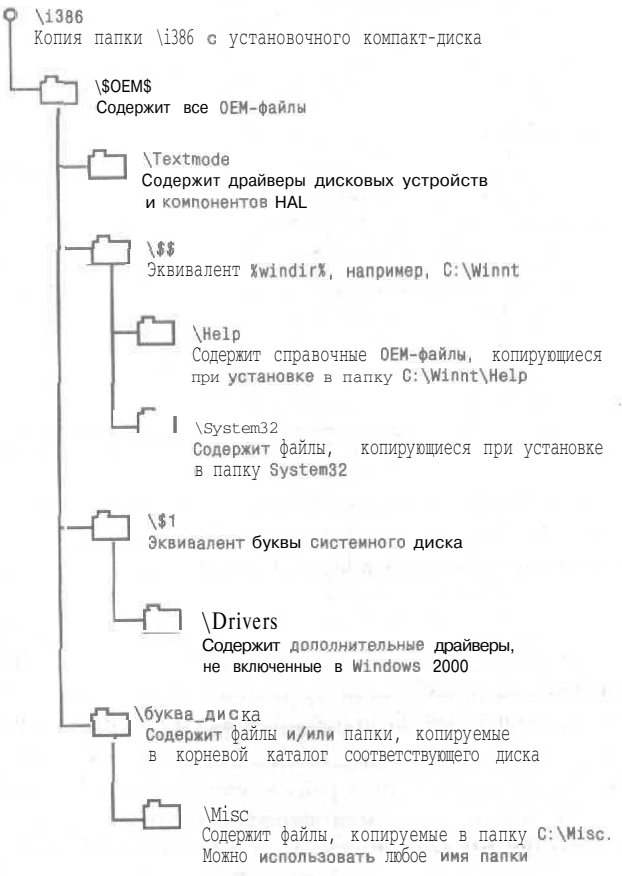


Рис. 3-1, Структура дистрибутивной папки

В \OEM создается структура папок для дополнительных файлов, копируемых на целевой компьютер при установке. Эти файлы включают драйверы, утилиты, приложения и другие файлы, необходимые для развертывания Windows 2000 Server.

\OEM может содержать необязательный файл Cmdlines.txt со списком команд, выполняемых во время графической стадии установки и использующихся для установки необязательных компонентов, например, утилит. Эти команды выполняются до регистрации в сети.

Обнаружив \SOEM$ в корне дистрибутива, Setup копирует найденные в этом каталоге файлы во временный каталог WIN_NT.~LS, созданный в период выполнения текстовой фазы. В процессе установки содержимое \$OEM$ копируется в соответствующие подпапки целевого компьютера. По завершении установки папки OEM и WIN_NT.~LS удаляются.

Примечание Все описанные ниже папки располагаются на дистрибутивном сетевом ресурсе в папке \OEM и копируются в различные каталоги на компьютере, выполняющем Setup.

\OEM\textmode

Копируется в $W1N_NT$.~BT. Содержит новые или измененные файлы для установки накопителей информации и специализированных уровней HAL. Эти файлы включают драйверы OEM уровней HAL для SCSI-устройств и файл Txtsetup.oem, управляющий загрузкой и установкой этих компонентов.

Список файлов, размещаемых в подпапке \OEM\textmode (слои HAL и драйверы), заносится в раздел [OEMBootFiles] файла ответов.

\$OEM$\$$

Копируется в %windir% и ее подпапки. Содержит файлы ОС (как новые, так и обновленные поставщиком), копируемые в разные подпапки при установке Windows 2000. Структура этой подпапки должна соответствовать структуре стандартной установки Windows 2000, где \$OEM$\$$ соответствует %windir%, \$OEM$\$$\System32 - %windir%\System32 и т. д. Каждая подпапка должна содержать файлы, которые будут копироваться в папки ОС на целевом компьютере.

Примечание В Windows 2000 переменная %systemroot% эквивалентна %windir%.

\$OEM$\$1

Копируется в $systemdrive$. Подпапка \$OEM$\$1 (новинка Windows 2000) указывает устройство, на котором установлена Windows 2000. $1 эквивалентно переменной %systemdrive%. Так, если Вы устанавливаете Windows 2000 на диск D:, \$OEM$\$1 укажет на него. Это позволяет устанавливать Windows 2000 не только на диск C:.

\$OEM$\$1\Drivers

Копируется в $systemdrive$\Drivers и подпапки $systemdrive$\Drivers. Появившаяся в Windows 2000 подпапка \$OEM$\$1\Drivers позволяет размещать в подпапке Drivers новые или измененные драйверы PnP-устройств и их дополнительные файлы (файлы каталога и INF-файлы установки). Эти папки вместе с содержимым копируются в папку %systemdrive%\Drivers целевого компьютера. Добавление в файл ответов параметра OemPnPDriversPath укажет Windows 2000, где искать новые или измененные драйверы PnP-устройств. При поиске соответствующих драйверов PnP-устройств, устанавливаемых во время или после установки, Windows 2000 ищет файлы в созданных Вами папках и в пап-

ках с драйверами, поставляемыми с системой. Имя драйвера можно поменять согласно формату 8.3 имен MS-DOS.

Примечание Подпапка \$OEM$\$1\Drivers заменяет подпапки \Display и \Net, используемые при установке Windows NT.

\$OEM$\$1\Sysprep

Копируется в %systemdrive%\Sysprep. Содержит файлы, необходимые для запуска утилиты Sysprep, для правильной работы которой требуется наличие файлов Sysprep.exe и Sysprepcl.exe в папке %systemdrive%\Sysprep.

Совет Добавьте файл Sysprep.inf (созданный при помощи Setup Manager или написанный вручную) в каталог \SOEM$\$l\Sysprep на дистрибутивном сетевом ресурсе, иначе для завершения установки Sysprep понадобится дискета с файлом Sysprep.inf.

\OEM*буква_диска*

На текстовом этапе установки структура каждой папки \$OEM$*буква_диска* копируется в корень соответствующего устройства целевого компьютера. Например, файлы из подпапки \$OEMS\D копируются в корневой каталог устройства D:. Точно так же можно создавать подпапки, например, \$OEM$\E\Misc заставит Setup создать подпапку Misc на устройстве E:.

Файлы, требующие переименования, перечисляются в файле $$Rename.txt. Заметьте, что файлы в дистрибутивных папках должны иметь короткие имена (формат 8.3).

Упражнение 1: подготовка и запуск автоматической установки

Запустите автоматическую установку Windows 2000 Server на Computer 2. На Server01 с помощью Setup Manager (Диспетчер установки) создайте файл ответов и дистрибутивный сетевой ресурс.

Внимание! Не меняйте параметры рабочего стола или любого приложения Windows 2000 Server на Server01.

▶ Задание 1: запустите Setup Manager

Выполняйте это упражнение на ServerOl, вставив в привод CD-ROM установочный компакт-диск Windows 2000 Server.

1. При помощи Windows Explorer (Проводник) создайте в папке C:\Program Files подпапку с именем Deploy.
2. С помощью Windows Explorer найдите на установочном компакт-диске Windows 2000 Server папку Support\Tools.
3. Выбрав в дереве каталогов папку Tools, дважды щелкните файл Deploy.cab в правой панели.

   Откроется содержимое архива Deploy.cab.
4. В меню Edit (Редактировать) выберите команду Select All (Выбрать все).
5. В меню File (Файл) выберите команду Extract (Извлечь).

   Откроется окно Browse For Folder (Обзор папок).
6. Откройте диск C:, щелкнув значок «+» слева от надписи Local Disk (C:) [Локальный диск (C:)].

7. Откройте папку Program Files.
8. Щелкните папку Deploy.

   Откроется одноименная папка.
9. Щелкните OK.

   Архив Deploy будет распакован в папку C:\Program Files\DepIoy.
10. В папке C:\Program Files\Deploy дважды щелкните значок программы setupmgr.

    Откроется окно программы Setup Manager и мастер Windows 2000 Setup Manager (Диспетчер установки Windows 2000).
11. Прочтите текстовое описание и щелкните кнопку Next (Далее).

    Откроется окно New Or Existing Answer File (Новый или существующий файл ответов) с выбранным переключателем Create A New Answer File (Создать новый файл ответов).
12. Щелкните кнопку Next.

    Откроется окно Product To Install (Устанавливаемый продукт) с выбранным переключателем Windows 2000 Unattended Installation (Автоматическая установка Windows 2000).
13. Щелкните Next.

    Откроется окно Platform (Платформа) с выбранным переключателем Windows 2000 Professional.
14. Выберите переключатель Windows 2000 Server и щелкните Next.

    Откроется окно User Interaction Level (Уровень взаимодействия с пользователем) с выбранным переключателем Provide Defaults (Предоставление значений параметров по умолчанию).
15. Выберите переключатель Fully Automated (Полностью автоматическая установка), прочтите описание и щелкните Next.

    Откроется окно License Agreement (Лицензионное соглашение).
16. Прочтите текст в окне, пометьте флажок I Accept The Terms Of The License Agreement (Я принимаю условия этого лицензионного соглашения) и щелкните Next.

    Откроется окно Customize The Software (Настройка принадлежности).
17. В поле Name (Имя) наберите Ваше имя и нажмите клавишу Tab.
18. В поле Organization (Организация) наберите название Вашей организации или **MSPress Self-Study** и щелкните Next.

    Откроется окно Licensing Mode (Режим лицензирования) с выбранным переключателем Per Server («На сервер»).
19. Выберите переключатель Per Seat («На рабочее место») и щелкните Next.

    Откроется окно Computer Names (Имена компьютеров).
20. Вставьте компакт-диск Windows 2000 Training Supplemental в привод CD-ROM на Server01 и щелкните кнопку Import (Импортировать).

    Откроется окно Open (Открыть).

21. В поле File Name (Имя файла) наберите *<привод_cd-rom:>*\chapt03\ex1\computer **names.txt и** щелкните кнопку Open (Открыть).

    Откроется окно Computer Names (Имена компьютеров) с перечнем устанавливаемых компьютеров.
22. Щелкните Next.

    Откроется окно Administrator Password (Пароль администратора).
23. В поле Password (Пароль) наберите **password** и пометьте флажок When The Computer Starts, Automatically Log On As Administrator (При загрузке компьютера автоматически войти как администратор).

Значение параметра Number of times to Auto Logon (Количество автоматических входов) — 1.

24. Щелкните Next,

    Откроется окно Display Settings (Параметры экрана).

25. Оставьте во всех списках значения Use Windows Default (Использовать умолчания Windows) и щелкните Next.

    Откроется окно Network Settings (Сетевые параметры) с выбранным переключателем Typical Settings (Типичные параметры).

26. Щелкните Next.

    Откроется окно Workgroup or Domain (Рабочая группа или домен) с выбранным переключателем Workgroup **(В** составе рабочей группы).

    Server01 сейчас входит в рабочую группу WORKGROUP, поэтому изменять значение в окне Workgroup or Domain (Рабочая группа или домен) не нужно. После запуска автоматической установки на Computer 2, он войдет в ту же группу. Позже ServerOl станет контролером домена, и тот компьютер, для которого Вы подготовите файл ответов, войдет в тот же домен.

Примечание Созданный сейчас файл ответов позднее можно изменить для входа в домен и создания в нем учетной записи компьютера. Это можно сделать с помощью Setup Manager или текстового редактора.

---

27. Щелкните Next.

    Откроется окно Time Zone (Часовой пояс)

28. В списке Time Zone (Часовой пояс) выберите Ваш часовой пояс и щелкните Next.

    Откроется окно Additional Settings (Дополнительные параметры) с выбранным переключателем Yes, Edit The Additional Settings (Да, настроить дополнительные параметры).

29. Щелкните Next.

    Откроется окно Telephony (Телефония).

30. Вы можете ввести коды страны, города и другие параметры, необходимые для исходящих звонков. Если у Вас нет модема, не заполняйте окно.

31. Щелкните Next.

    Откроется окно Regional Settings (Язык и стандарты) с выбранным переключателем Use The Default Regional Settings For The Windows Version You Are Installing (Выбрать региональные стандарты, используемые по умолчанию для устанавливаемой версии Windows).

32. Щелкните Next.

    Откроется окно Languages (Языки).

33. Выберите дополнительные языки, поддержка которых Вам нужна для работы в Windows 2000 Server, и щелкните Next.

    Откроется окно Browser and Shell Settings (Параметры обозревателя и оболочки) с выбранным переключателем Use Default Internet Explorer Settings (Использовать для настройки обозревателя параметры по умолчанию).

34. Щелкните Next.

    Откроется окно Installation Folder (Папка установки) с выбранным переключателем A Folder Named Winnt (В папку с именем Winnt).

35. Щелкните Next.

    Откроется окно Install Printers (Установка принтеров).

36. Щелкните Next.
    Откроется окно Run Once (Однократное выполнение).
37. В поле Command To Run (Команда) наберите **Notepad.exe** и щелкните кнопку Add (Добавить).
    Обычно в поле Command To Run (Команда) указывается сценарий или другая программа, выполняющая настройку пользовательского окружения. Нам достаточно запустить Notepad (Блокнот).
38. Щелкните Next.
    Откроется окно Distribution Folder (Дистрибутивная папка).
39. Выберите переключатель Yes, Create Or Modify A Distribution Folder (Да, создать или изменить дистрибутивную папку) и щелкните Next.
    Откроется окно Distribution Folder Name (Имя дистрибутивной папки) с выбранным переключателем Create A New Distribution Folder (Создать новую дистрибутивную папку).
    В поле Distribution Folder (Дистрибутивная папка) будет указано C:\win2000dist, а в поле Share As (Использовать как общий ресурс) — win2000dist.
40. Щелкните кнопку Next (Далее).
    Откроется окно Additional Mass Storage Drivers (Дополнительные запоминающие устройства).
41. Прочитайте описание и щелкните Next.
    Откроется окно Hardware Abstraction Layer (Слой абстрагирования оборудования).
42. Прочитайте описание и щелкните Next.
    Откроется окно Additional Commands (Дополнительные команды).
43. Прочитайте описание и щелкните Next.
    Введенные здесь команды записываются в файл Cmdlines.txt в дистрибутивной папке в подпапке OEM.
    Откроется окно OEM Branding (Фирменная установка).
44. Щелкните Next.
    Откроется окно Additional Files Or Folders (Дополнительный файлы или папки).
45. Шелкая папки, просмотрите их содержание.
    Щелкните Next.
    Откроется окно Answer File Name (Имя файла ответов).
46. Убедитесь, что имя файла соответствует C:\Win2000dist\Unattend.txt, и щелкните Next.
    Откроется окно Location Of Setup Files (Размещение файлов установки) с выбранным переключателем Copy The Files From CD (Копировать файлы с компакт-диска).
47. Смените в приводе компакт-диск Windows 2000 Server Training Supplemental (прилагаемый к книге) на установочный компакт-диск Windows 2000 Server.
48. Закройте окно автозапуска компакт-диска Windows 2000 Server.
49. В окне Location Of Setup Files (Размещение файлов установки) щелкните Next.
    При копировании фалов из каталога \i386 установочного компакт-диска в папку C:\Win2000Dist откроется окно Copying Files (Копирование файлов).
50. Дождитесь завершения копирования файлов.
    Откроется окно мастера Completing The Windows 2000 Setup Manager Wizard (Завершение работы мастера диспетчера установки Windows 2000).
51. Щелкните кнопку Finish (Готово).

► **Задание 2: изучите созданную Setup Manager дистрибутивную папку**

Проанализируйте структуру созданной Setup Manager папки, файлы ответов (Unattend.txt), UDF (Unattend.udf) и командный файл (Unattend.bat).

1. В меню Start (Пуск) выберите команду Run (Выполнить).
   Откроется диалоговое окно Run (Запуск программы).
2. В поле Open (Открыть) наберите **C:\Win2000dist** и щелкните кнопку OK,
   Откроется окно Win2000dist.
3. Откройте другое окно для папки *<буква cd-rom:>*\i3S6 на установочном компакт-диске Windows 2000.
   Откроется окно i386.
4. Расположите окна так, чтобы одновременно видеть win2000dist и i386.
5. Какая папка, отсутствующая в i386, появилась в папке Win2000dist?
6. Проанализируйте структуру каталога в папке oem, используя рис. 3-1 в этом тексте.
7. Вернитесь в папку Win2000dist и найдите Unattend-файлы.
   Заметьте, что у двух Unattend-файлов расширения не показаны.
8. Для просмотра расширений у всех файлов, выберите в меню Tools (Сервис) команду Folder Options (Свойства папки).
   Откроется одноименное окно.
9. Щелкните вкладку View (Вид).
10. В списке Advanced Settings (Дополнительные параметры) сбросьте флажок Hide File Extensions For Known File Types (Скрывать расширения для зарегистрированных типов файлов) и щелкните кнопку OK.

И. Снова найдите файлы с именами Unattend.
   Теперь они показаны с расширениями. Щелкните Unattend.txt и в меню File — команду Open (Открыть).
   В окне Notepad отобразится содержимое Unattend.txt.

12. Найдите раздел [UserData] и добавьте в него дополнительную строку с именем ProductID+*<ключ_Вашего_продукта>*. В качестве значения параметра ProductID наберите код Вашей копии Windows 2000 Server,
13. Сохраните и закройте файл Unattend.txt.
14. Подробности о разделах этого файла см. в файле Unattend.doc, расположенном в папке C:\Program Files\Deploy, созданной в начале упражнения 2. Файл Unattend.doc можно открыть в программах Microsoft Wordpad, Microsoft Word и других текстовых процессорах, понимающих формат файлов Microsoft Word.
15. Закройте файл Unattend.doc.
16. В окне Win2000dist щелкните файл Unattend.udf, а затем в меню File (Файл) выберите команду Open With (Открыть с помощью).
   Откроется окно Open With (Выбор программы).
17. В списке Choose The Program You Want To Use (Выберите программу, которую Вы хотите использовать) выберите Notepad и щелкните кнопку OK.
   Убедитесь, что файл содержит 12 имен компьютеров, импортированных во время работы Setup Manager.

38. Для чего нужны UDF-файлы?
19. Закройте UDF-файл.
20. В окне Win2000dist щелкните файл Unattend.bat, а затем в меню File (Файл) выберите команду Edit (Изменить).

Откроется программа Notepad с содержимым этого файла.

21. Убедитесь, что файл залает переменные, используемые для запуска Winnt32 с ключами. Заметьте также, что при вызове командного файла Вам нужно указывать имя компьютера, так как UDF-файл включен в подпрограмму установки.
22. Закройте файл Unattend.bat.

► **Задание 3: запустите автоматическую установку Windows 2000 Server на Computer 2**

На Computer 2 установите 32-разрядную версию ОС Windows, например Windows 95 или Windows NT. Server01 и Computer 2 подключите в одну сеть.

Внимание! Если Computer 2 работает под управлением Windows NT и имеет загрузочный раздел C:\ и каталог ОС с именем Winnt, измените имя установочного каталога в файле Unattend.txt. Имя каталога указано в разделе Unattended в переменной TargetPath. Введите, например, TargetPath=\WIN2000S.

---

1. На Computer 2 подключите сетевой диск (в этом упражнении для него будет использована буква H:) к \\Server01\WIN2000dist. К ServerOl можно подключиться, используя имя Administrator и пароль password.

   Примечание Если при работе в Windows 9x возникают проблемы с подключением к ServerOl, проверьте, входит ли компьютер в группу WORKGROUP и войдите в систему как Administrator (Администратор) с паролем password.

   ---

2. В командной строке наберите cd H:.

   Внимание! Если Вы обновляли Windows 9x, программа установки может не найти UDF-файл. В этом случае откройте файл Unattend.txt на ServerOl и укажите полный путь к UDF-файлу.

   ---

3. В командной строке наберите H:\Unattend Server02.
4. Откроется окно Copying Installation Files (Копирование установочных файлов), и Windows 2000 Server запустит автоматизированную установку по сети.

   По завершении этой фазы появится запрос о перезагрузке компьютера.

   Примечание Эту стадию установки можно выполнить, используя ключ \syspart при вызове Winnt32.exe.

   ---

5. Перезагрузите компьютер.

   После перезагрузки откроется меню загрузки Windows 2000, и установка Windows 2000 Server продолжится в текстовом режиме.

   Компьютер перезагрузится снова, и появится меню загрузки с выбранным пунктом Windows 2000 Server,

   Установка Windows 2000 продолжится в графическом режиме. Для завершения установки потребуется время. Затем Вам будет предложено перезагрузить компьютер.
6. Перезагрузив компьютер, убедитесь, что был произведен автоматический вход в систему с учетной записью администратора, как это было указано в Setup Manager. На этой стадии будет запущена программа Notepad.exe.
7. Закройте Notepad (Блокнот).

   Откроется окно Windows 2000 Configure Your Server (Настройка сервера Windows 2000).

8. **Щелкните переключатель I** Will **Configure** This Server Later, **а затем — кнопку** Next. Откроется окно **Configure Your Server (Настройка** сервера).
9. Сбросьте флажок Show This Screen At Startup (Открывать это окно при загрузке) и закройте окно.

Внимание! При обновлении с Windows 9x в качестве файловой системы должна быть выбрана NTFS. Если этого не было сделано, преобразуйте имеющуюся файловую систему в NTFS, введя в командной строке convert c: /fs:ntfs.

Резюме

Перед выполнением автоматической установки Windows 2000 Server нужно создать файл ответов — специализированный сценарий, содержащий ряд необязательных разделов, которые Вы можете изменять. Файл предоставляет Setup ответы на все вопросы, которые задаются пользователю при ручной установке. Файл ответов также указывает Setup способ взаимодействия с созданными Вами установочными файлами/папками. Для сетевой установки Windows 2000 Server надо создать минимум один набор дистрибутивных папок. Утилита Setup Manager (Диспетчер установки) позволяет автоматически или вручную создать дистрибутивную папку и файл ответов. О дальнейшей настройке файла ответов см. файл Unattend.doc на установочном компакт-диске Windows 2000 Server.

Занятие 2. Автоматизация установки Windows 2000 Server

Автоматическая установка Windows 2000 Server подразумевает запуск Setup с файлом ответов. Установку в автоматическом режиме можно выполнять на множестве компьютеров. Автоматизируется установка:

- собственно ОС Windows 2000 Server;
- любого приложения, не запускаемого как служба;
- дополнительной языковой поддержки Windows 2000 для различных языковых пакетов;
- пакетов обновлений Windows 2000 Server.

Мы рассмотрим автоматическую установку Windows 2000 Server. Автоматической установке других приложений посвящено занятие 3.

Изучив материал этого занятия, Вы сможете:

✓ автоматически установить Windows 2000 Server.

Продолжительность занятия - около 45 минут.

Выполнение автоматической установки

Для выполнения автоматической установки надо указать файл ответов при запуске Setup. Windows 2000 Server автоматически устанавливается тремя основными способами: с загрузочного компакт-диска, при помощи программ Winnt.exe или Winnt32.exe.

Загрузочный компакт-диск

Для автоматической установки Windows 2000 Server этим способом:

- компьютер должен поддерживать формат El Torito Bootable CD-ROM (не в режиме эмуляции) для загрузки с привода компакт-дисков;
- файл ответов должен иметь имя Winnt.sif и располагаться на дискете, которую вставляют в дисковод после загрузки компьютера с компакт-диска;
- файл ответов должен содержать раздел [Data] с необходимыми параметрами.

Winnt.exe или Winnt32.exe

Пример вызова команды Winnt.exe для автоматической установки:

```
Winnt /s:Z:\i386 /u:Z:\unattend.txt /t:c
```

Ключ /и: в командной строке задает автоматическую установку. Ключ /t: указывает устройство, на которое Setup скопирует файлы для продолжения установки. Z:\i386 — сетевой ресурс, содержащий установочные файлы Windows 2000. Перед выполнением этой команды на локальном компьютере надо подключить сетевой диск Z: к сетевому ресурсу, содержащему подпапку i386. Команда Winnt32.exe используется аналогично Winnt:

```
Winnt32 /s:Z:\i386 /unattend 10:Z:\unattend.txt /tempdrive:C
```

Для запуска автоматической установки Winnt32.exe использует ключ /unattend:. Число после ключа /unattend: задает время ожидания перед перезагрузкой компьютера и продолжением установки. Числовые команды работают в Windows NT или в Windows 2000, но не в Windows 9x.

Следующие шаги необходимы для запуска приведенных выше команд автоматической установки (рис. 3-2).

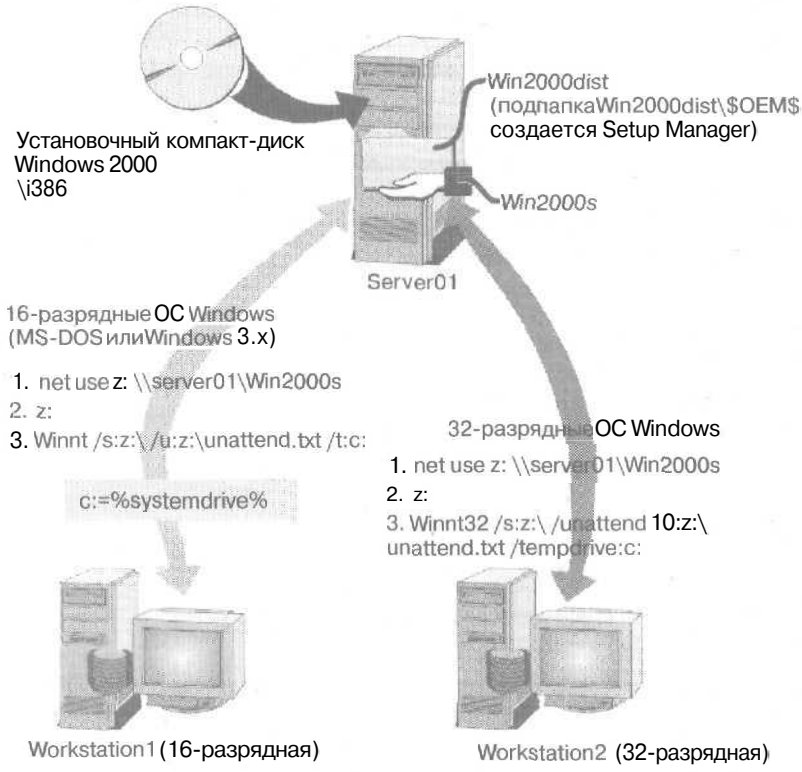


Рис. 3-2. Запуск автоматической установки на компьютерах под управлением 16- и 32-разрядных ОС

Автоматизация установки Windows 2000 Server

Осуществляется несколькими способами — выбор зависит от желаемого результата. Иногда эти способы можно комбинировать, например, совместно использовать утилиты Syspart и Sysprep.

Помимо рассмотренных выше способов, Windows 2000 Server можно автоматически установить с помощью:

- программы установки Winnt32.exe с ключом /syspart;
- утилиты Sysprep;
- Systems Management Server (SMS);
- загрузочного компакт-диска;
- службы удаленной установки Remote Installation Service (RIS).

Способ установки	Назначение	Обновление ОС	Новая установка ОС
Syspart	Служит для установки ОС на компьютеры с несовпадающими аппаратными конфигурациями.	Нет	Да

(окончание)

Способ установки	Назначение	Обновление ОС	Новая установка ОС
Sysprep	**Применяется при совпадении аппаратных конфигураций** у исходного и целевых компьютеров, включая HAL и накопители.	**Нет**	**Да**
Загрузочный компакт-диск	Применяется на компьютерах, допускающих загрузку с компакт-диска.	Нет	Да
RIS (Remote Installation Service)	Применяется на компьютерах, поддерживающих предзагрузочное выполнение (Pre-Boot Execution Environment, PXE) или загрузочные RIS-дискеты. Позволяет компьютеру подключиться к сетевому RIS-серверу в начале загрузки и получить от него установку Windows 2000 Professional. PXE позволяет компьютеру с ПЗУ загружаться с сетевого сервера. Код ПЗУ PXE может располагаться в ПЗУ BIOS или сетевой платы.	Да	Да
SMS	Служит для выполнения управляемых обновлений Windows 2000 Server на различных системах, особенно в случаях их географической разбросанности.	Да	Да

Примечание Как уже говорилось, RIS может автоматизировать установку только Windows 2000 Professional; с Windows 2000 Server эта служба не работает. Поддержка автоматической установки Windows 2000 Server и других ОС появится, вероятно, в следующих версиях RIS.

Выше рассматривались способы установки, используемые для обновления Windows NT Server или полной установки. Поэтому решите, чего именно Вы хотите. Автоматическая установка может заменить существующие файлы или разделы, так как выполняется без вмешательства пользователя. Файлы приложений и данных могут остаться на разделах диска, но для работы в новой ОС их нужно перерегистрировать.

Утилита Syspart

Syspart запускается как параметр программы Winnt32.exe. Winnt32 с ключом Syspart запускается на эталонном компьютере для завершения первой фазы Setup. Syspart применяют, если эталонный и целевые компьютеры имеют разные аппаратные конфигурации. Это сократит время развертывания за счет копирования установочных файлов на эталонном компьютере, что позволяет исключить данный этап при установке ОС на целевых компьютерах.

Syspart требует два физических диска с главным разделом на целевом жестком диске. Впрочем, целевой диск на исходном компьютере можно не устанавливать — это может быть любой компьютер в сети с чистым, без ОС диском.

Если нужно выполнить одинаковую установку и настройку ОС на компьютерах с разными типами HAL и накопителей, создайте с помощью Syspart исходный набор файлов, содержащий данные о конфигурации и драйверах. Затем его можно использовать и на несходных между собой системах для правильного определения оборудования и согласованной настройки основных частей ОС.

Запустив эталонный компьютер, подключитесь к дистрибутивной папке и активизируйте Setup из командной строки:

```
winnt32 /unattend:unattend.txt /s:источник_установки
syspart:цель_установки /tempdrive:цель_установки /noreboot
```

Цель_установки здесь соответствует D. После выполнения команды на диске D: будет создана такая структура (рис. 3-3):

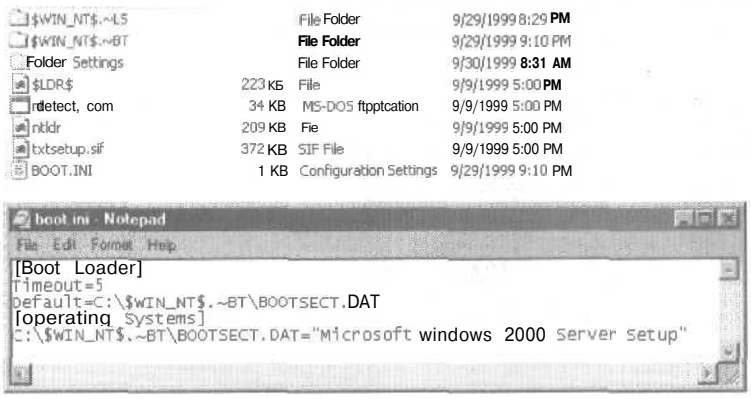


Рис. 3-3. Содержимое диска D: целевого компьютера и файла Boot.ini после запуска Syspart

Ниже приведены значения параметров, используемые при запуске Winnt32.exe.

- Значение Unattend.txt указывает на используемый файл ответов. Он содержит ответы на вопросы, на которые пользователь отвечает при установке. При создании исходного набора файлов применять файл ответов не обязательно.
- Значение *источник_установки* указывает на расположение файлов Windows 2000 Server. Если Вы хотите вести установку с нескольких источников одновременно, укажите в командной строке несколько ключей /s. На рис. 3-4 изображено одновременное копирование файлов из двух источников. Первый является сетевым диском, второй — локальным приводом CD-ROM. Можно задать до 8 источников установки,
- Параметры /syspart и /tempdrive должны указывать на один и тот же раздел второго жесткого диска. Установка Windows 2000 Server будет производиться на его главный раздел. Утилита Syspart помечает этот раздел активным для загрузки ОС.
- Параметр /tempdrive необходим для работы Syspart. Для успешной установки проверьте, хватит ли на главном разделе второго диска места для Windows 2000 Server и установочных файлов, расположенных в папке WIN_NT.~LS.
- Значение *установочный_диск* указывает на раздел, содержащий предустановку Windows 2000 Server. Файлы с этого диска показаны на рис. 3-3.

Примечание Syspart автоматически активизирует устройство при подготовке к его установке на целевой компьютер.

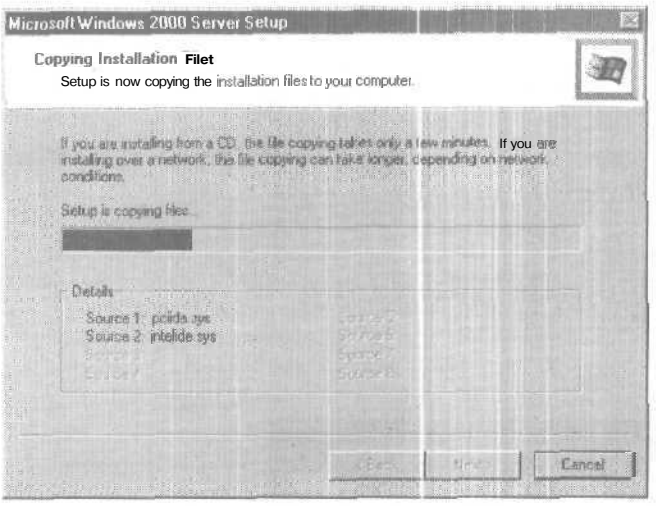


Рис. 3-4. Окно Copying Installation Files (Копирование файлов) с двумя источниками установочных файлов

Утилита Sysprep

Упрощает создание образа диска установки Windows 2000 Server. Дублирование дисков удобно для одинакового конфигурирования нескольких компьютеров. Чтобы задействовать Sysprep, на эталонный компьютер надо установить Windows 2000 Server и все приложения, которые будут использоваться па целевых компьютерах. Запустите Sysprep, а затем — программу копирования образа диска стороннего поставщика. Sysprep подготовит жесткий диск на исходном компьютере, чтобы утилита копирования образа смогла перенести его на другие компьютеры. Этот способ значительно ускоряет развертывание в сравнении с обычной установкой или установкой с применением сценариев.

Совет Создайте компакт-диск с образом диска или поместите образ на сетевой ресурс, чтобы использовать его для установки ОС на одинаковых или похожих компьютерах.

Для использования Sysprep, исходный и целевые компьютеры должны иметь одинаковые HAL, поддержку ACPI и накопители. Когда компьютер стартует после установки, PnP-устройства определяются повторно. Эго означает, что PnP-устройства, например сетевые, звуковые и видеоплаты, у эталонного и целевых компьютеров могут не совпадать. Главное преимущество установки ОС с помощью Sysprep — скорость. Образ, включающий необходимые для распространяемой конфигурации файлы, можно упаковать и сжать. Добавляются и драйверы, которые могут понадобиться в других системах. Образ можно скопировать на компакт-диск для распространения в удаленных сайтах, подключенных по медленным каналам связи.

Примечание Поскольку эталонный и целевые компьютеры должны иметь одинаковые HAL, поддержку ACPI и накопители, требуются несколько образов диска для удовлетворения всем возможным конфигурациям.

Sysprep позволяет создать исходный образ, содержащий компоненты для рядовых серверов. Затем Вы можете настроить сервер и повысить его до контролера домена. Это мож-

но сделать вручную или включив команды в раздел [GuiRunOnce] файла Sysprep.inf. О файле Sysprep.inf см. также раздел «Файлы Sysprep» этой главы.

Если у Вас несколько типов аппаратно-зависимых систем, при создании образов для каждого типа можно вместе с Sysprep вызвать Syspart. Для этого установите Windows 2000 на один из компьютеров каждого типа и с помощью Sysprep создайте образы для установки ОС на оставшихся компьютерах каждого типа.

Перед началом работы выберите эталонный компьютер — на нем должна быть установлена Windows NT Server или Windows 2000 Server.

Примечание Sysprep можно применять и для установки Windows 2000 Professional.

Работа Sysprep

Ниже рассказано о подготовке исходного компьютера для дублирования посредством Sysprep.

- **Установка Windows 2000.** На исходном компьютере с аппаратной конфигурацией, как у целевых компьютеров, надо установить Windows 2000 Server. При этом компьютер не нужно включать в домен. Не заполняйте пароль локального администратора.
- **Настройка компьютера.** Для установки и настройки Windows 2000 Server и связанных с ним приложений надо войти в систему с правами администратора. Можно установить IIS или установить и настроить другие службы.
- **Проверка образа.** Чтобы проверить правильность настройки образа, настройте аудит клиента согласно Вашим требованиям. Затем удалите всю ненужную информацию, включая журналы событий и результаты аудита.
- **Подготовка образа к дублированию.** Убедившись, что компьютер настроен верно, систему можно готовить для дублирования: запустите Sysprep с применением необязательного файла Sysprep.inf (о нем см. ниже в этом разделе). Когда Sysprep сделает свое дело, компьютер автоматически завершит работу или сообщит о готовности к выключению.
- **Дублирование установки.** К этому моменту жесткий диск компьютера готов к распознаванию PnP-устройств, созданию уникального SID и запуску мастера мини-установки после перезагрузки системы. Перед выполнением следующей фазы установки жесткий диск дублируется утилитами сторонних фирм, например, Norton Utilities Ghost или PowerQuest Drive Image Pro 3.0. Следующая загрузка Windows 2000 Server произойдет с данного жесткого диска или с любого другого, который создан из этого образа, система определит PnP-устройства, создаст уникальный SID и запустит мастер мини-установки для завершения установки и настройки на целевом компьютере.

Внимание! Связанные с Active Directory компоненты копированию не подлежат. Не создавайте на рядовом сервере объекты локальных пользователей и групп, поскольку новым учетным записям не будут назначены новые SID.

Файлы Sysprep

Для использования Sysprep запустите файл Sysprep.exe вручную или настройте Setup для автоматического запуска Sysprep.exe, используя раздел [GuiRunOnce] файла ответов. Для запуска Sysprep файлы Sysprep.exe и Setupcl.exe должны находиться в папке Sysprep в корневом каталоге системного диска (%systemdrive%\Sysprep\). Для правильного расположения файлов при установке добавьте их в подпапку OEM\$1\Sysprep\.

Файлы Sysprep готовят ОС для клонирования и запускают мастер мини-установки. Необязательный файл ответов Sysprep.inf можно включить в папку Sysprep. Он содержит

параметры по умолчанию для ответов на вопросы, что сокращает пользовательский ввод и тем самым исключает потенциальные ошибки. Sysprep.inf можно разместить на дискете, которую вставляют после появления диалога загрузки системы. После успешного завершения работы мастера мини-установки система в последний раз перезагружается, папка Sysprep удаляется вместе с содержимым — компьютер готов к регистрации пользователя.

Файлы Sysprep делятся на следующие разделы.

Sysrep.exe — имеет три необязательных параметра:

Параметр	Описание
–quiet	Запускает Sysprep без вывода сообщений на экран.
–nosidgen	Запускает Sysprep без регенерации имеющихся в системе SID. Это полезно, когда не требуется клонировать компьютер, на котором запускается Sysprep.
-reboot	Автоматически перезагружает компьютер по завершении работы Sysprep. Этот параметр вызывает перезагрузку системы по окончании дублирования диска, чтобы автоматически запустить Mini-Setup (версию Setup, запускаемую после дублирования образа на жесткий диск). Этот ключ применяется только при аудите процесса Sysprep, чтобы убедиться в корректности работы мастера мини-установки.

Sysrep.inf — файл ответов, применяемый при клонировании для обеспечения уникальной настроечной информацией каждого целевого компьютера. Использует синтаксис, подобный .INI-файлам, и имена параметров, как в файле ответов для Setup (unattend.txt). Sysprep.inf разместите в папке %systemdrive%\Sysprep\ или на дискете, которую надо вставить сразу после появления меню загрузки системы — в это время идет поиск измененного файла Sysprep.inf. Если же Sysprep.inf не включить при работе Sysprep, мастер мини-установки будет выводить на экран все свои диалоговые окна.

Если Sysprep.inf используется при настройке эталонного компьютера с уже запущенной Sysprep, для предоставления другого файла Sysprep.inf используйте дискету, Пути к системным файлам, необходимым Mini-Setup, например, OEMPnPDriversPath и InstallFilesPath, для файла Sysprep.inf дистрибутивной папки и файла Sysprep.inf на дискете должны совпадать.

Пример файла Sysprep.inf:

```
[Unattended]
;Заставьте пользователя принять лицензионное соглашение.
OemSkipEula - No
;Использовать умолчания Sysprep и регенерировать файл подкачки
;для устранения потенциальных различий в объеме ОЗУ.
KeepPageFile = 0
;Путь к файлам языковой поддержки.
;которые могут понадобиться в международных организациях.
InstallFilesPath = %systemroot%\Sysprep\i386

[GuiUnattended]
;Задание непустого пароля администратора.
;Любой заданный здесь пароль будет работать,
;если в исходном образе (на эталонном компьютере) задан непустой пароль.
;В противном случае пароль, используемый на исходном компьютере,
;будет использоваться и на целевом. Его можно будет изменить только вручную,
```

```
;войдя в систему как локальный администратор.
AdminPassword = ABC123
;Задание часового пояса.
TimeZone - 20
;Пропуск окна приветствия после загрузки системы.
OemSkipWelcome = 1
;Не пропускать диалог настройки региональных параметров.
;чтобы с ними ознакомился пользователь.
OemSkipRegional=No

[UserData]
;Информация о пользователе системы
FullName - «Авторизованный пользователь»
OrgName - "Название организации»
ComputerName = XYZ_Computer1

[GUIRunOnce]
;Сделать данный компьютер контролером домена после перезагрузки
DCPromo

[Identification]
;Включить компьютер в домен ITDOMAIN
JoinDomain = ITDOMAIN

[Networking]
;Привязать стандартные протоколы и службы к сетевой плате этого компьютера.
InstallDefaultComponents = Yes
```

Изменить пароль администратора в Sysprep.infможно, если существующий пароль пуст. Это относится и к изменению пароля через графический интерфейс Sysprep. О разделах файла ответов и командах, применяемых в Sysprep.inf, см. приложение Б на прилагаемом компакт-диске.

Setupcl.exe обрабатывает файл Sysprep.inf для ответов на вопросы мастера мини-установки и запускает мастер Mini-Setup.

Примечание Программы Sysprep.exe и Setupcl.exe заменили утилиту Rollback.exe из предыдущих версий Windows NT.

***Мастер** мини-установки*

Запускается при первой загрузке компьютера с диска, дублированного с помощью Sysprep. Мастер собирает сведения для последующей настройки целевого компьютера. Если Вы не используете Sysprep.inf или не заполнили некоторые его разделы, мастер мини-установки задаст все вопросы, ответов на которые нет в Sysprep.inf.

Мастер мини-установки выводит окна, для пропуска которых надо задать соответствующие параметры в Sysprep.inf:

Окно	Значение параметра
Лицензионное соглашение	[Unattended] OemSkipEula = Yes
Язык и стандарты	[RegionalSettings] LanguageGroup = 1 Language = 00000409
Имя пользователя и название организации	[UserData] FullName = «Имя пользователя» OrgName= «Название организации»
Имя компьютера и пароль администратора	[UserData] ComputerName = W2B32054 [GuiUnattended] AdminPassword — «password»
Сетевые параметры	[Networking] InstallDefaultComponents = Yes
Параметры TAPI	[TapiLocation] AreaCode = 425
Выбор часового пояса	OEMSkipRegional = 1 TimeZone = 20

Так как Setup определяет оптимальные параметры экрана, окно их настройки не отображается при работе Setup или мастера мини-установки. Параметры экрана можно задать в файле ответов, используемом при настройке эталонного компьютера, или в файле Sysprep.inf, который будет применяться на целевом компьютере. Параметры экрана, заданные в файле ответов, изменятся, если в Sysprep.inf будут указаны другие значения или в системе будут обнаружены видеоплата или монитор другого типа.

Если параметр OemSkipEula равен Yes, Вы берете на себя ответственность за принятие лицензионного соглашения от имени пользователя.

При запуске Setup по сети с применением Sysprep надо настроить сетевые платы иначе, чем при использовании параметра InstallDefaultComponents. В файле Sysprep.inf надо указать сведения о сети. При наличии DHCP достаточно установить клиент для сетей Microsoft, протокол TCP/IP и службу доступа к файлам и принтерам для сетей Microsoft. При этом в Sysprep.inf дополнительно ничего указывать не нужно.

Запуск Sysprep

Sysprep можно запустить вручную и автоматически.

Запуск Sysprep вручную

После установки Windows 2000 Server утилиту Sysprep используют для подготовки переноса системы на другие компьютеры аналогичной конфигурации. Для запуска Sysprep вручную надо установить Windows 2000 Server, настроить систему и установить приложения, затем вызвать Sysprep без ключа –reboot. После выхода из системы образ диска клонируют на компьютеры аналогичной конфигурации.

Примечание Утилита Sysprep находится в архиве Deploy.cab в каталоге \Support\Tools на установочном компакт-диске Windows 2000 Server.

При первой загрузке клонированного компьютера запускается мастер мини-установки, с помощью которого пользователи дополнительно настраивают свои компьютеры. Вы

можете переопределить все или часть конфигурационных параметров Sysprep в файле Sysprep.inf. По завершении работы мастера мини-установки папка Sysprep (с программами Sysprep.exe и Setupcl.exe) автоматически удаляется.

Подготовка установки Windows 2000 Server для дублирования осуществляется, как описано ниже.

- **Подготовка папки Sysprep.** В папку Sysprep в корневом каталоге диска копируются файлы Sysprep.exe, Setupcl.exe и при необходимости файл Sysprep.inf.
- **Запуск утилиты Sysprep.** Утилита Sysprep запускается из командной строки в папке Sysprep одной из команд:

```
Sysprep
Sysprep -reboot
Sysprep /<необязательный параметр>
Sysprep /<необязательный параметр> -reboot
Sysprep /<необязательный параметр 1>s/<необязательный
параметр X>
Sysprep /<необязательный параметр 1>s/<необязательный
параметр X> -reboot
```

- **Запуск Sysprep без ключа –reboot.** Увидев сообщение о завершении работы компьютера, выберите в меню Start (Пуск) команду Shut Down (Завершение работы). Затем для создания образа установки надо задействовать утилиту копирования образа диска,
- **Запуск Sysprep с ключом -reboot.** После автоматической перезагрузки компьютера запустится мастер мини-установки. Протестируйте его работу. Можно включить аудит системы и приложений. Завершив аудит, запустите Sysprep из командной строки без ключа –reboot. Увидев сообщение о необходимости завершения работы компьютера, выберите в меню Start (Пуск) команду Shut Down (Завершение работы). Затем для создания образа установки задействуйте утилиту копирования образа диска.

Примечание Можно добавить файл Cmdlines.txt в папку Sysprep для его обработки Setup. Этот файл позволяет выполнять команды по завершении установки, включая программы установки приложений.

Автоматический ***запуск Sysprep***

Раздел [GuiRunOnce] файла ответов содержит команды, выполняемые после установки. Его используют для завершения установки, автоматического входа в систему, запуска Sysprep и завершения работы компьютера.

Для автоматического запуска файлы Sysprep надо добавить в дистрибутивные папки в OEM\$1\Sysprep\, что обеспечит их копирование в нужные места системного диска. Последней командой в разделе [GuiRunOnce] должна быть;

```
%systemdrive%\Sysprep\Sysprep.exe -quiet
```

Если требуется несколько перезагрузок, ее надо добавить вслед за последней командой последнего раздела [GuiRunOnce].

Если компьютер поддерживает APM или ACPI, Sysprep автоматически закончит работу компьютера по завершении этого процесса.

Расширение разделов диска с помощью Sysprep

В Windows 2000 расширение разделов происходит в графическом режиме. Вы можете создавать образы дисков, которые можно расширить, если жесткий диск целевого компьютера больше, чем на эталонном. Это позволяет уменьшить размер образа, когда он не за-

нимает весь диск, и увеличить объем используемого дискового пространства. Графический интерфейс облегчает доступ к данной возможности Sysprep.

Если применяемая утилита позволяет редактировать образ, можно удалить хранящиеся в нем файлы Pagefile.sys, Setupapi log и Hyberfil.sys (если таковые есть), поскольку они будут созданы заново при запуске мастера мини-установки на целевом компьютере. На работающем компьютере эти файлы удалять нельзя.

Для расширения раздела жесткого диска при использовании утилит работы с образом диска, поддерживающих NTFS, надо сначала установить минимальный размер раздела жесткого диска исходного компьютера, необходимый для установки Windows 2000 Server с необходимыми компонентами и приложениями. Это позволит уменьшить требования к общему размеру образа. Надо также изменить файл ответов, используемый для создания исходного образа, включив в раздел [Unattended] параметр FileSystem = ConvertNTFS. Включать сюда ExtendOemPartition не нужно, так как Вам надо получить образ минимального размера. Затем на эталонном компьютере можно установить Windows 2000 Server и создать образ диска. Оттуда можно перенести образ на целевой компьютер при совпадении размеров их системных разделов. После перезагрузки целевого компьютера и запуска мастера мини-установки раздел сразу расширится.

Systems Management Server

Systems Management Server (SMS) применяется для управляемых обновлений Windows 2000 Server на нескольких системах, особенно если они удалены географически. SMS служит только для установки на компьютеры с ОС и клиентским агентом SMS, который и обрабатывает инструкции по установке ПО. Перед обновлением посредством SMS надо оценить структуру сети, включая пропускную способность, аппаратуру и географические ограничения. Главное преимущество SMS — возможность централизованного управления процессом обновления. Например, можно задать момент проведения обновления (во время обучения, после проверки оборудования или по завершении резервного копирования пользовательских данных), обновляемые компьютеры и способ применения сетевых ограничений.

SMS 2.0 содержит файлы пакетов (с расширением .sms), позволяющие импортировать установочные подпрограммы Windows 2000 Server в SMS 2.0. После импорта определения пакета укажите SMS путь к установочному компакт-диску Windows 2000 или сетевому ресурсу с дистрибутивом Windows 2000 Server.

Применение загрузочного компакт-диска

Для установки Windows 2000 Server на компьютере, BIOS которого допускает загрузку с компакт-диска, можно использовать загрузочный компакт-диск. Этот способ применяется на компьютерах удаленных сайтов, с медленными каналами связи или при отсутствии квалифицированных специалистов. *С* загрузочного диска запускается Winnt32.exe и выполняет установку.

Примечание Загрузочный компакт-диск применяется только для установки на чистый жесткий диск. Для выполнения обновлений надо запускать Winnt32.exe в существующей ОС.

Для достижения максимальной гибкости при установке Windows 2000 Server настройте в BIOS следующий порядок загрузки:

- сетевая плата — этот параметр применяется для совместимых с PXE ПЗУ в целях поддержки установки ОС с RIS-сервера;
- CD-ROM — для установки ОС с загрузочного компакт-диска;

- **жесткий диск** — для подготовки установки ОС с помощью Sysprep или Syspart;
- **дискета** — для установки ОС с дискет.

Для полностью автоматической установки ОС с загрузочного компакт-диска соблюдайте следующие условия:

- BIOS компьютера должна поддерживать формат El Torito для загрузки с CD-ROM (не в режиме эмуляции);
- файл ответов должен содержать раздел [Data] с необходимыми параметрами;
- файл ответов назовите Winnt.sif и поместите на дискете.

Порядок установки Windows 2000 Server с загрузочного компакт-диска таков.

- **Загрузка системы.** Вставьте в привод CD-ROM компакт-диск Windows 2000 Server и перезагрузите компьютер.
- **Загрузка файла Wmnt.sif.** После перезагрузки стартует текстовый режим установки Windows 2000. Дискета с файлом Wmnt.sif должна быть вставлена в дисковод. Когда она будет считана, выньте ее. Установка продолжится с компакт-диска, как указано в файле Wmnt.sif.

Примечание На загрузочном компакт-диске должны находиться необходимые файлы. UDF-файлы при этом использовать нельзя, так как для каждой установки при указании UDF-файла из Winnt.exe или Winnt32.exe вызывается уникальный идентификатор.

Резюме

Автоматически установить Windows 2000 Server можно четырьмя способами. Команда Winnt32.exe с параметром Syspart применяется при несовпадении аппаратуры эталонного и целевых компьютеров. В этом случае для автоматической установки используют утилиту Sysprep, которая упрощает создание образа диска установки Windows 2000 Server. Следующий способ — использовать SMS для выполнения управляемых обновлений Windows 2000 Server на нескольких системах, особенно при их географической удаленности. SMS используется только для установки на компьютеры, имеющие ОС и клиентский агент SMS. Наконец, автоматическую установку можно выполнить с загрузочного компакт-диска. Это удобно при установке ОС на компьютеры удаленных сайтов с медленными каналами связи или при отсутствии квалифицированных специалистов.

Занятие 3. Автоматизация установки серверных приложений

Наряду с Windows 2000 Server можно автоматизировать и установку других приложений на целевые компьютеры. Это делается с помощью файла Cmdlines.txt или файла ответов. Cmdlines.txt содержит список команд, выполняемых во время графической стадии установки Windows 2000. В файл ответов для этого включается раздел [GuiRunOnce], куда добавляют программу установки приложений или командный файл.

Изучив материал этого занятия, Вы сможете:

- ✓ выполнять автоматическую установку серверных приложений с помощью файла Cmdlines.txt;
- ✓ использовать для этого раздел [GuiRunOnce] файла ответов.

Продолжительность занятия — около 35 минут.

Файл Cmdlines.txt

Cmdlines.txt содержит команды, выполняемые во время графической стадии процесса установки. Программа установки активизирует их при установке необязательных компонентов, например приложений, которые надо установить сразу после Windows 2000 Server. Планируя применение Cmdlines.txt, поместите его в подпапку \OEM дистрибутивной папки.

Файл Cmdlines.txt используется:

- при установке компонентов из подпапки \OEM дистрибутивной папки;
- при установке приложений, изначально не готовых для совместной работы, например Microsoft Office 95, или разработанных для индивидуальной работы с последующей репликацией сведений о пользователях;
- если надо войти в систему в качестве службы и реплицировать изменения для всех пользователей.

Синтаксис Cmdlines.txt:

```
[Commands]
"<команда_1>"
"<команда_2>"
"<команда_x>"
```

Параметры *<команда_1>*, *<команда_2>* и *<команда_x>* — это метки для команд, которые надо выполнить в указанном порядке при работе Setup в графическом режиме. Заметьте: все команды заключаются в кавычки.

Cmdlines.txt выполняется как служба, а не в результате вызова зарегистрированным пользователем. В итоге устанавливаемые приложения регистрируются в общем реестре, и их смогут запускать все пользователи системы. Кроме того, все указанные в Cmdlines.txt файлы для запуска приложений или утилит должны содержаться в дистрибутивных папках.

Файл ответов

Раздел [GuiRunOnce] файла ответов содержит список команд, выполняемых при первом входе пользователя в систему по завершении установки. Например, для автоматического запуска Sysprep в фоновом режиме в раздел [GuiRunOnce] добавьте команду:

```
[GuiRunOnce]
Command ()="%systemdrive%\Sysprep\Sysprep -quiet"
```

Примечание **Чтобы** параметры **были применены** для **всех пользователей,** запустите Sysprep **из раздела [GuiRunOnce].**

Новой возможностью при использовании раздела [GuiRunOnce] является доступ к переменным окружения, как это показано выше. Впрочем, Вы по-прежнему вправе использовать полные пути.

Используя для установки раздел [GuiRunOnce], предусмотрите возможную перезагрузку системы устанавливаемым приложением и предотвратите ее. Это важно, так как при каждой перезагрузке предыдущие строки данного раздела для однократного запуска игнорируются. Если система перезагрузится раньше, чем завершатся предыдущие команды из раздела [GuiRunOnce], оставшиеся команды не выполнятся.

Если предотвратить перезагрузку нельзя, измените размещение приложений в пакетах MSI или установочных пакетах SMS. С Windows 2000 Server поставляется программа VERITAS WinINSTALL LE, а с SMS 2.0 - SMS Installer.

Альтернативный способ — переместить команды установки утилит и приложений, вызывающих перезагрузку, в конец раздела [GuiRunOnce]. Для этого перед перезагрузкой добавьте дополнительные записи в реестр, чтобы Windows 2000 выполнила следующий набор команд. Первой выполняемой в этом разделе должна быть команда редактирования реестра:

```
regedit /$ <имя_файла.reg>
```

где <*имя_файла*.reg> указывает файл реестра, позволяющий выполнить желаемые действия при нескольких перезагрузках. При этом в первой строке каждого файла <*имя_файла* reg> должна стоять команда загрузки из раздела RunOnce следующего набора параметров реестра, пока не будут выполнены все нужные команды.

Для автоматического входа в систему в качестве администратора надо задать параметр AutoAdminLogonCount. Автоматический вход поддерживается не более чем для 99 перезагрузок. В файле ответов для установки Windows 2000 надо также указать пароль локального администратора.

Примечание При установке приложений на разные языковые версии Windows 2000, рекомендуется протестировать работоспособность распакованных приложений: правильно ли размещаются их файлы и модифицируется реестр.

Если для установки приложения нужна оболочка Microsoft Windows Explorer (Проводник), раздел [GuiRunOnce] использовать нельзя, так как эта программа не загружается на этапе выполнения команд из разделов файла ответов. Запросите у поставщика программы обновление или исправление, позволяющее обойтись без Windows Explorer. В противном случае можно упаковать приложение в MSI-пакет или задействовать другое средство распространения.

Приложения с однотипным механизмом установки могут неправильно работать, если не указать команду /wait. Сбои происходят, когда запускается еще одна установка приложения до завершения предыдущей. Так как запускается несколько экземпляров однотипной программы установки, часто установка уже второго приложения неудачна.

Установка приложений

Для установки приложений при помощи раздела [GuiRunOnce] файла ответов применяют два способа: запуск программы установки приложения и командный файл.

Программы установки приложений

Предпочтительным методом для установки приложений является использование установочных программ, поставляемых с приложением. Это можно сделать, если приложения допускают установку без вмешательства пользователя. Фоновый режим обычно требует применять ключи /q или /s в командной строке. Список поддерживаемых установочным механизмом параметров командной строки см. в справочном файле приложения или его документации.

Вот пример команды из раздела [GuiRunOnce] для автоматической установки приложения. Заметьте: используется собственная программа установки:

```
<путь к программе установки>\Setup.exe /q
```

Параметры в зависимости от приложений могут различаться. Так, параметр /1 позволяет создать файл отчета для контроля установки. Некоторые приложения имеют команды, автоматически запрещающие перезагрузку. Это полезно для установки приложений с минимальным количеством перезагрузок. Запросите у поставщика соответствующие инструкции и утилиты.

Примечание Примите лицензионные соглашения всех приложений независимо от способа их установки.

Командный файл

Чтобы установить несколько приложений, создайте командный файл с индивидуальными установочными командами, запускающий Windows 2000 из командной строки с ключом /wait. Его можно запускать из раздела [GuiRunOnce] файла ответов. Это гарантирует последовательную и полную установку каждого приложения.

Ниже описано создание командного файла установки приложения и удаления всех ссылок на командный файл по завершении установки.

- **Создание командного файла.** В нем должны быть примерно такие строки:

  ```
  Start /wait <путь>\<команда установки> <параметры командной строки>
  Start /wait <путь>\<команда установки> <параметры командной строки>
  Exit
  ```

  где:

  - *<путь>* — путь к исполняемому файлу программы установки; он должен быть доступен в момент установки.
  - *<команда установки>* — имя команды установки.
  - *<параметры командной строки>* — любые параметры фонового режима, которые использует устанавливаемое приложение.

- **Копирование командного файла.** Командный файл надо скопировать в дистрибутивную папку или другой доступный во время установки ресурс. При использовании Sysprep во время установки Windows 2000 командный файл копируют в подпапку Sysprep *в* дистрибутивные папки. В результате на целевом компьютере он будет расположен локально. При включении компьютера после запуска Sysprep и завершения работы мастера мини-установки папка Sysprep удаляется вместе с содержимым. Удалять файл из других процессов не требуется.

- **Добавление командного файла к файлу ответов.** Ссылку на командный файл добавляют в раздел [GuiRunOnce] файла ответов.
- **Копирование LNK-файла на эталонный компьютер.** Файл .lnk копируется с эталонного компьютера в папки OEM\$1\documents and settings\all users\start menu\programs\startup. После перезагрузки и запуска графического интерфейса происходит установка приложений с последующим удалением файла .lnk из группы Startup (Автозагрузка).

Резюме

Для автоматизации установки серверных приложений применяется два способа. Первый из них — выбрать файл Cmdlines.txt с командами, выполняемыми в графическом режиме установки. Setup выполняет эти команды при установке необязательных компонентов. Второй способ — редактирование раздела [GuiRunOnce] файла ответов, содержащего команды, выполняемые при первом входе пользователя в систему по завершении установки. При использовании для установки файла ответов можно применять установочные программы, поставляемые с приложением, либо создать командный файл с конкретными установочными командами.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Для чего применяются ключи /tempdrive: и /t: программ Winnt32.exe или Winnt.exe?

2. Вам надо разработать стратегию быстрой установки Windows 2000. После оценки условий выделились три категории компьютеров, требующих установки Windows 2000 Server:
   - 30 одинаковых компьютеров с Windows NT Server 4.0, которые нужно обновить до Windows 2000;
   - 20 одинаковых компьютеров, на которых надо выполнить новую установку Windows 2000 Server;
   - на удаленных сайтах будет выполнена установка Windows 2000 Server на чистые диски; надо обеспечить установку Windows 2000 Server со стандартного образа, соответствующего настройке Вашей локальной ОС; для этого нужно предоставить жесткие диски для их установки на удаленные серверы.

   Перечислите этапы Вашей стратегии установки.

3. Для чего Setup Manager (Диспетчер установки) создает папку OEM и ее подпапки?

4. Чем отличается установка с помощью файла Cmdlines.txt от установки с помощью раздела [GuiRunOnce] файла ответов?

5. Чем отличаются утилиты Syspart и Sysprep?

ГЛАВА 4

Файловые системы Microsoft Windows 2000

В этой главе

Windows 2000 поддерживает файловые системы NTFS, FAT16 и FAT32, а также файловые системы только чтения CDFS (CD-ROM File System) и UDF (Universal Disk Format). Эта глава посвящена файловым системам **NTFS,** FAT16 и FAT32.

NTFS и FAT различаются структурой томов и организацией файлов. В Windows 2000 используется NTFS 5.O. Эта файловая система обладает дополнительными возможностями, не реализованными в FAT и только частично реализованными в NTFS для Windows NT 4.0. В этой главе обсуждается обслуживание жестких дисков, файловые системы FAT и NTFS, проблемы безопасности файлов и папок в этих системах.

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить требования, описанные в разделе «Об этой книге»; на Computer 1 должно быть 500 Мб неразмеченного дискового пространства на диске 0;
- выполнить упражнения глав 2 и 3 — на обоих компьютерах должен быть установлен и настроена ОС Windows 2000 Server.

Занятие 1. Обслуживание жестких дисков

Перед установкой Windows 2000 Server надо определить структуру той части жесткого диска, которая будет использоваться *ОС,* разбить ее на разделы и отформатировать. Если системный и загрузочный разделы будут разделены, необходимо разбить на разделы и отформатировать обе области диска — на которой содержится ОС и с системными файлами. Мы обсудим настройку и обслуживание дисков.

Изучив материал этого занятия, Вы сможете:

- ✓ описать концепцию обслуживания дисков;
- ✓ сформулировать основные задачи обслуживания дисков;
- ✓ создать и настроить динамический диск.

Продолжительность занятия — около 60 минут.

Настройка жесткого диска

При настройке свободного пространства на жестком диске или жесткого диска, предназначенного для Windows 2000, надо:

- инициализировать диск — определить фундаментальную структуру диска; Windows 2000 поддерживает два типа дисков: базовый и динамический;
- создать разделы или тома — Вы должны разбить на разделы базовый диск или создать тома на динамическом диске;
- отформатировать диск — созданный раздел или том надо отформатировать под одну из файловых систем (NTFS, FAT16 или FAT32); выбор файловой системы отразится на способах контроля доступа пользователей к данным, хранения данных, производительности диска и ОС, которые смогут получить доступ к данным.

Типы дисков, разделов и томов

Прежде чем приступить к настройке жесткого диска, познакомимся с типами дисков, разделов и томов, поддерживаемыми Windows 2000.

Типы дисков

Windows 2000 поддерживает два типа дисков; базовый и динамический. Первый может быть либо базовым, либо динамическим. В многодисковых системах можно использовать диски обоих типов (рис. 4-1).

Примечание Тип дисков Windows 2000 надо отличать от аппаратных дисковых массивов. RAID-массив сначала отображается в Windows 2000 как неразмеченное пространство, которое затем можно настроить как базовое или динамическое хранилище.

Базовый диск

Это промышленный стандарт. Такой диск делится на *разделы* (partition) — части, функционирующие как физически отдельные устройства хранения данных. Windows 2000 поддерживает два типа разделов: основной и дополнительный. Базовый диск может содержать основные и дополнительные разделы и логические диски. Вновь установленный диск в Windows 2000 инициализируется как базовый.

Так как базовая структура диска является стандартом, ее поддерживают MS-DOS и все версии Microsoft Windows/NT/2000. По умолчанию Windows 2000 использует базовую структуру диска, которую можно преобразовать в динамическую.

Базовые диски совместимы с наборами томов Windows NT, чередующимися наборами (RAID-0), зеркальными (RAID-1) и чередующимися с четностью (RAID-5) томами.

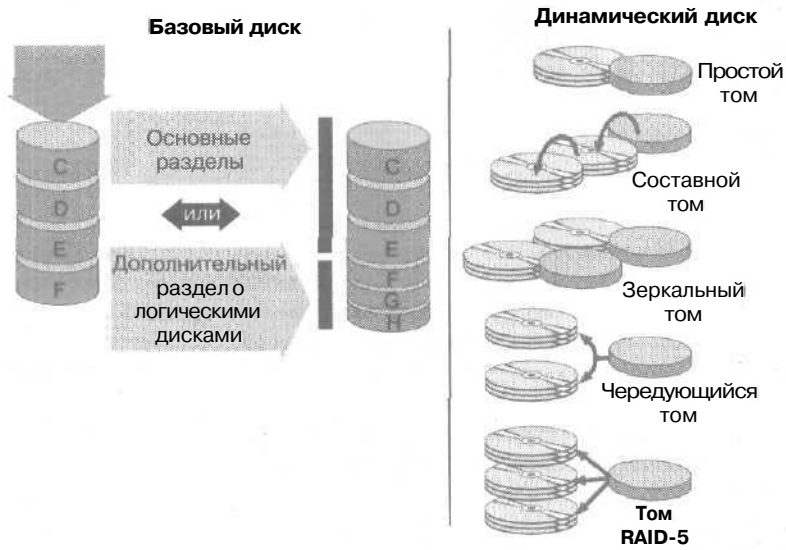


Рис. 4-1. Базовый и динамический диски

Динамический диск

Поддерживается только в Windows 2000. Динамическая структура подразумевает создание одного раздела, занимающего все дисковое пространство.

Динамические диски делятся на тома, включающие области на одном или нескольких физических дисках. Динамический диск может содержать простые, составные, чередующиеся (RAID-0), зеркальные (RAID-1) и чередующиеся с четностью (RAID-5) тома. Динамический диск создается путем модернизации базового диска.

Динамическая структура диска позволяет обойти некоторые ограничения базовых дисков, например, можно установить или изменить объем динамического диска, не перезагружая компьютер.

Примечание Съемные накопители могут содержать только основные разделы. На них нельзя создать дополнительные разделы, логические диски или динамические тома. Основной раздел на съемных накопителях не может быть активным.

Типы разделов (для базовых дисков)

Жесткий диск можно разбить на основной и дополнительный разделы. Каждый раздел — это изолированная секция для хранения данных. Разделы позволяют хранить различные типы информации раздельно, например, пользовательские данные на одном и приложения на другом разделе. Базовый диск может содержать до 4 основных или до 3 основных разделов и один дополнительный раздел. Иначе говоря, максимальное количество разделов всегда равно 4, при этом только один раздел может быть дополнительным (рис. 4-2).

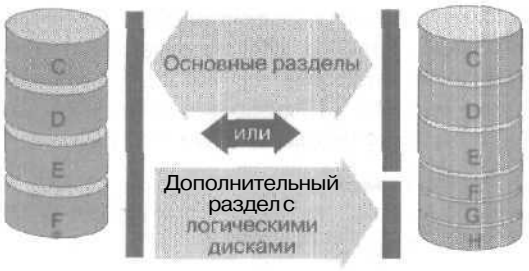


Рис. 4-2. Типы разделов

Основные разделы

Windows 2000 использует основные разделы для запуска компьютера. Один из основных разделов должен быть помечен как активный. *Активный раздел* (active partition) хранит загрузочные файлы и применяется для запуска ОС. В каждый момент времени только один основной раздел на одном жестком диске может быть активным. Несколько основных разделов позволяет изолировать разные ОС или типы данных. Для альтернативной загрузки Windows 2000 с Microsoft Windows 95 или MS-DOS активный раздел должен быть отформатирован под FAT16, так как Windows 95 не считывает разделы, отформатированные под FAT32 или NTFS. Для альтернативной загрузки с Microsoft Windows 95 OSR2 (более поздняя версия Windows 95, поддерживающая FAT32) или Windows 98 активный раздел должен быть отформатирован под FAT16 или FAT32.

Совет Если активный раздел отформатирован в NTFS, Windows 9x может быть запущена с дискеты. Дискета содержит указатель на раздел FAT, на котором находится Windows 9x.

Системный раздел (system partition) Windows 2000 (или системный том) — это активный раздел, содержащий файлы для загрузки ОС. *Загрузочный раздел* (boot partition) Windows 2000 — это основной раздел или логический диск, на котором установлены файлы ОС. Загрузочный и системный разделы могут занимать один раздел. Впрочем, системный раздел должен находиться на активном разделе (обычно это диск C:), тогда как загрузочный раздел может располагаться на другом основном или дополнительном разделе.

Дополнительные разделы

Дополнительный раздел (extended partition) может быть создан из оставшейся части свободного места. На жестком диске может быть только один дополнительный раздел, поэтому оптимально задействовать все оставшееся свободное место для создания дополнительного раздела. В отличие от основных дополнительный раздел можно не форматировать и не обозначать буквой алфавита. Дополнительный раздел разбивается на сегменты — логические диски. Вы должны дать имя логическому диску и отформатировать его с помощью одной из файловых систем.

Типы томов (для динамических дисков)

Базовый диск можно модернизировать до динамического и затем создать тома Windows 2000. При этом надо определить, какой тип тома подходит Вам для эффективного использования дискового пространства и отказоустойчивости. *Отказоустойчивость* (fault tolerance) ~ это способность компьютера или ОС обойтись без потерь данных в случае сбоя. В Windows 2000 отказоустойчивыми являются тома RAID-1 и RAID-5.

Простой том

Простои том (simple volume) — это дисковое пространство на одном жестком диске. Простой том может занимать несколько областей (до 32) на одном диске. Отказоустойчивости он не обеспечивает. Данные в нем еще более уязвимы, поскольку чем больше размер простого тома, тем выше вероятность потери информации из-за отказа любого из его разделов.

Составной том

Составной том (spanned volume) включает в себя пространство нескольких дисков (до 32). При записи данных на составной том Windows 2000 полностью заполняет сначала первый диск, затем второй и делает то же со всеми дисками в томе. Составной том отказоустойчивым не является. Поломка одного из дисков влечет потерю данных всего тома.

Зеркальный том

Зеркальный том (mirrored volume) состоит из двух одинаковых копий простого тома, каждая из которых находится на отдельном жестком диске. Зеркальные тома повышают отказоустойчивость при сбое жесткого диска.

Чередующийся том

Чередующийся том (striped volume), или RAID-0, объединяет области свободного пространства нескольких дисков (до 32) в один логический том. При работе с чередующимся томом Windows 2000 оптимизирует выполнение, записывая данные на диски равномерно. Если сломается один из дисков чередующегося тома, теряются данные всего тома. Поэтому, как простые и составные тома, том RAID-0 отказоустойчивости не обеспечивает.

Том RAID-5

Отказоустойчив. Windows 2000 добавляет блоки контрольных сумм на каждый диск тома; эти блоки позволяют восстановить данные тома при отказе какого-либо жесткого диска. Создание тома RAID-5 требует минимум 3 жестких дисков.

Ограничения, **накладываемые на динамические диски и тома**

Динамические диски, обладающие меньшей отказоустойчивостью, чем простой, дополнительный простой, составной или чередующийся том, не могут содержать загрузочный и системный разделы. Эта особенность встроена в Windows 2000, чтобы обеспечить базовый уровень отказоустойчивости для разделов, содержащих файлы ОС. Динамические диски могут быть прочитаны только из Windows 2000. Так что динамические диски неприменимы при альтернативной загрузке другой ОС. Динамические тома не используются в портативных компьютерах. Отказоустойчивые конфигурации (RAID-1 и RAID-5) нельзя создать локально на компьютерах с Windows 2000 Professional.

Файловые системы

Windows 2000 работает с файловыми системами NTFS, FAT16 и FAT32, поддерживающими чтение и запись данных. Разделы NTFS и FAT поддерживают как базовые, так и динамические диски, но если раздел должен обеспечивать защиту на уровне файлов и папок, сжатие, квотирование или шифрование, надо применять NTFS. Только Windows 2000/NT могут получить доступ к данным на логическом диске, отформатированном под NTFS. Если Вы собираетесь сделать сервер контроллером домена, отформатируйте установочный раздел под NTFS. Это связано с тем, что NTFS поддерживает некоторые важные серверные функции, например, службы Active Directory и RIS.

FAT16 и FAT32 совместимы с другими ОС. Для альтернативной загрузки Windows 2000 и другой ОС отформатируйте системный раздел под FAT16 или FAT32. FAT не обладает некоторыми возможностями NTFS, например, защитой на уровне файлов, поэтому обыч-

но следует форматировать жесткий диск под NTFS. Единственная причина использования FAT16 или FAT32 — альтернативная загрузка. О файловых системах FAT и NTFS см. занятия 2 и 3.

Основные задачи обслуживания дисков

Информация о дисках и основные задачи их обслуживания, например, создание и удаление разделов и томов, включены в оснастку Disk Management (Управление дисками). Имея соответствующие права, можно обслуживать диски локально или с удаленного компьютера.

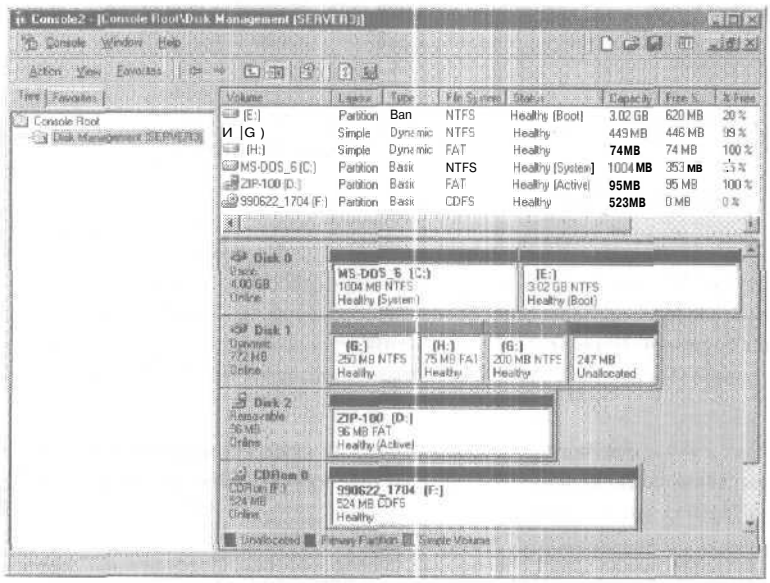


Рис. 4-3. Оснастка Disk Management (Управление дисками)

Вы можете настроить собственную консоль MMC и добавить к ней оснастку Disk Management. Эта оснастка также включена в стандартную консоль Computer Management (Управление компьютером). Чтобы открыть ее, в программной группе Administrative Tools (Администрирование) щелкните ярлык Computer Management (Управление компьютером). Disk Management отображает контекстные меню с командами, которые можно выполнить над выделенным объектом, и включает утилиты, упрощающие модернизацию дисков и создание разделов и томов.

Оснастка Disk Management отображает сведения о дисках в виде таблицы или графика. Режим просмотра меняется командами меню View (Вид).

Помимо мониторинга информации о дисках, Disk Management позволяет выполнять такие задачи, как установка и удаление жесткого диска и изменение типа диска. На рис. 4-4 показано, как можно преобразовать базовый диск в динамический.

Работа с простыми томами

Простой том представляет собой пространство одного диска. Простой том может быть расширен за счет неразмеченного пространства на том же диске. Простые тома не являются отказоустойчивыми, но можно создать два простых тома, которые будут содержать одни и те же данные. Простой том можно отформатировать под NTFS, FAT16 или FAT32, однако расширение допускает только NTFS.

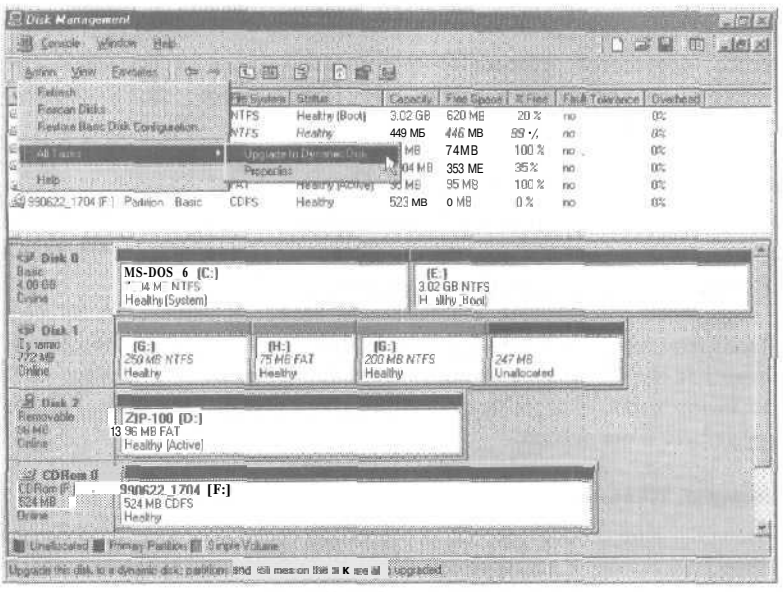


Рис. 4-4. Преобразование базового диска в динамический

Для создания простого тома в оснастке Computer Management раскройте узел Storage (Запоминающие устройства) и щелкните папку Disk Management. Щелкните правой кнопкой неразмеченное пространство динамического диска, на котором надо создать новый том и выберите в контекстном меню команду Create Volume (Создать том). Откроется окно мастера Create Volume (Мастер создания тома) — он проведет Вас через все этапы создания простого тома.

Чтобы расширить простой том NTFS, щелкните его значок правой кнопкой и выберите в контекстном меню команду Extend Volume (Расширить том). Откроется окно мастера расширения тома. Выполните его инструкции, чтобы расширить простой том за счет неразмеченного пространства любого динамического диска. Если при расширении используется пространство другого диска, простой том превращается в составной.

Работа с составными томами

Составной том включает в себя пространство нескольких дисков и позволяет использовать его более эффективно. Для создания составного тома требуется минимум два динамических диска. Составные тома не могут быть частью зеркального или чередующегося тома и не являются отказоустойчивыми.

Объединение свободного пространства для создания составного тома

Составной том создается объединением областей свободного пространства нескольких дисков (от 2 до 32) в один большой логический том. Области свободного пространства, входящие в составной том, могут быть разного размера. Организация составных томов в Windows 2000 такова, что данные записываются сначала на первый диск до его заполнения, затем то же происходит со вторым диском. Этот процесс повторяется для каждого следующего диска (их может быть до 32).

Путем удаления небольших томов и объединения освободившегося пространства в один составной том можно освободить буквы дисков и создать один большой том.

Примечание Все конфигурации динамических дисков в Windows 2000 допускают применение контроллеров разных технологий, изготовителей и моделей. Так, один динамический диск составного тома может быть подключен к контроллеру IDE, а другой — к контроллеру SCSI.

Дополнение и удаление

Отформатированный под NTFS составной том допускает расширение за счет свободного места. Оснастка Disk Management форматирует новую область, не затрагивая данных исходного тома. Том с FAT16 или FAT32 расширить нельзя.

При дополнении составного тома можно использовать до 32 динамических дисков. Том, расширенный пространством нескольких дисков, превращается в составной и не может быть задействован как часть зеркального или чередующегося тома. Ни одна часть расширенного тома не может быть удалена без удаления всего составного тома. Расширить системные и загрузочные тома нельзя.

Работа с чередующимися томами

Чередующиеся тома имеют лучшие скоростные характеристики среди всех подходов управления дисками в Windows 2000 Server. В таких томах данные записываются равномерно по всем жестким дискам порциями по 64 кб. Поскольку все жесткие диски чередующегося тома выполняют те же функции, что и один диск, Windows 2000 может параллельно выполнять команды ввода-вывода на всех дисках, а значит, чередующиеся тома ускоряют ввод-вывод.

Чередующийся том создается путем объединения областей свободного пространства нескольких дисков (2–32) в один логический том. Как и с составными томами, при работе с чередующимися, Windows 2000 записывает данные на несколько дисков. Однако на чередующихся томах ОС распределяет файлы равномерно по всем дискам. Как и составные, чередующиеся тома не отказоустойчивы. При поломке одного из дисков теряются данные всего тома.

Для создания чередующегося тома надо иметь минимум 2 динамических диска. Максимально для создания чередующегося тома можно использовать 32 диска. В дальнейшем Вы не сможете расширить или сделать зеркальным чередующийся том. Для создания чередующегося тома служит оснастка Disk Management. Щелкнув правой кнопкой неразмеченное пространство динамического диска, где надо создать чередующийся том, выберите в контекстном меню команду Create Volume (Создать том) — откроется окно мастера создания тома.

Добавление дисков

Новые диски в Windows 2000 инициализируются как базовые.

Добавление нового диска

Установите или присоедините новый физический диск (или Диски), а затем в оснастке Disk Management в меню Action (Действие) выберите команду Rescan Disks (Повторить сканирование дисков). Эту команду надо выполнять каждый раз, когда Вы удаляете или устанавливаете диск. Обычно при установке нового диска перезагружать компьютер не нужно. Но это надо сделать, если Disk Management не может обнаружить новый диск после выполнения Rescan Disks.

Установка диска, снятого с другого компьютера

Перенос диска с одного компьютера на другой отличается от установки нового диска. После переноса диска надо использовать оснастку Disk Management. Чтобы добавить новый диск, щелкните его правой кнопкой и выберите в контекстном меню команду Import Foreign Disk (Импорт чужих дисков) — откроется окно соответствующего мастера.

Установка нескольких дисков, снятых с другого компьютера

То же самое, что перенос одного диска. Чтобы добавить несколько зависимых дисков, снимите их с одного компьютера, установите на другой и в оснастке Disk Management укажите группу добавляемых дисков.

При переносе динамического диска будут доступны все его тома. Впрочем, если том занимает несколько дисков и один из них не был перенесен на новый компьютер, оснастка Disk Management этот том не отобразит.

Изменение типа диска

Базовый диск можно модернизировать в динамический. При этом все существующие разделы преобразуются в простые тома. Все зеркальные, чередующиеся, составные наборы, созданные в Windows NT 4.0, становятся соответственно зеркальными, чередующимися, составными томами динамического диска. Чередующийся том с четностью преобразуется в том RAID-5.

Для успешной модернизации каждый диск должен содержать 1 Мб неразмеченного пространства. Перед модернизацией диска надо закрыть все обращающиеся к нему программы. Вот результаты преобразования базового диска в динамический:

Организация базового диска	Организация динамического диска
Системный раздел	Простой том (не может быть расширен)
Загрузочный раздел	Простой том (не может быть расширен)
Основной раздел	Простой том
Дополнительный раздел	Простой том для каждого логического диска и оставшегося неразмеченного пространства
Логический диск	Простой том
Набор томов	Составной том
Чередующийся набор	Чередующийся том
Зеркальный набор	Зеркальный том
Чередующийся набор с четностью	Том RAID-5

Примечание Перед преобразованием диска сделайте копию данных.

Модернизация базового диска в динамический

Базовый диск можно модернизировать в динамический: щелкните правой кнопкой значок базового диска и выберите в контекстном меню команду Upgrade To Dynamic Disk (Обновление до динамического диска). Откроется окно мастера обновления. По завершении процесса перезагрузите компьютер.

Преобразовав базовый диск в динамический, Вы сможете создавать тома, обладающие дополнительными возможностями, но диск не сможет содержать основные или дополнительный разделы. Доступ к динамическим дискам можно получить только из Windows 2000.

Обратное преобразование динамического диска в базовый

Перед преобразованием динамического диска надо удалить все тома, чтобы все пространство диска считалось неразмеченным. Чтобы преобразовать динамический диск в базовый, щелкните правой кнопкой динамический диск (все неразмеченное пространство) и выберите в контекстном меню команду Revert To Basic Disk (Восстановить конфигурацию базового диска).

Внимание! При преобразовании динамического диска в базовый все данные будут потеряны.

Просмотр и обновление информации

Основные параметры выбранного диска можно просмотреть в диалоговом окне его свойств.

Свойства диска

В оснастке Disk Management в панели с графическим представлением диска щелкните правой кнопкой имя диска (но не его том) и выберите в контекстном меню команду Properties (Свойства) (рис. 4-5).

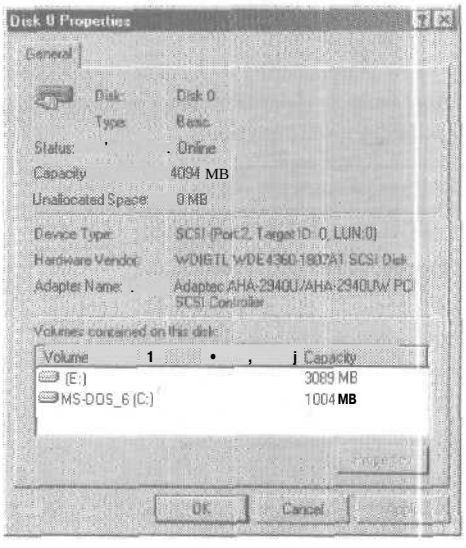


Рис. 4-5. Свойства диска О

В диалоговом окне свойств диска отображаются следующие свойства.

Категория	Описание
Disk (Диск)	Системный номер диска, например Disk0, Disk1, Disk2 и т. д.
Type (Тип)	Тип диска (базовый, динамический или съемный).
Status (Состояние)	Подключенный, выключенный, посторонний или неизвестный.
Capacity (Емкость)	Общий объем диска.
Unallocated Space (Незанятое место)	Объем незанятого дискового пространства. Здесь не показывается свободное пространство разделов базовых дисков или томов динамических дисков.

(окончание)

Категория	Описание
Device Type (Тип устройства)	IDE, SCSI или улучшенный IDE (EIDE). Также показывает канал IDE (основной или дополнительный), к которому подключен диск IDE, и порт, целевой идентификатор и номер LUN для дисков с интерфейсом SCSI.
Hardware Vendor (Поставщик)	Изготовитель и тип диска.
Adapter Name (Адаптер)	Тип контроллера, к которому подключен диск.
Volumes contained (Тома, находящиеся на данном диске)	Тома на данном диске и их общий объем.

Свойства тома

Чтобы просмотреть свойства тома в оснастке Disk Management, щелкните том правой кнопкой и выберите в контекстном меню команду Properties (Свойства). На рис. 4-6 изображено диалоговое окно свойств локального тома.

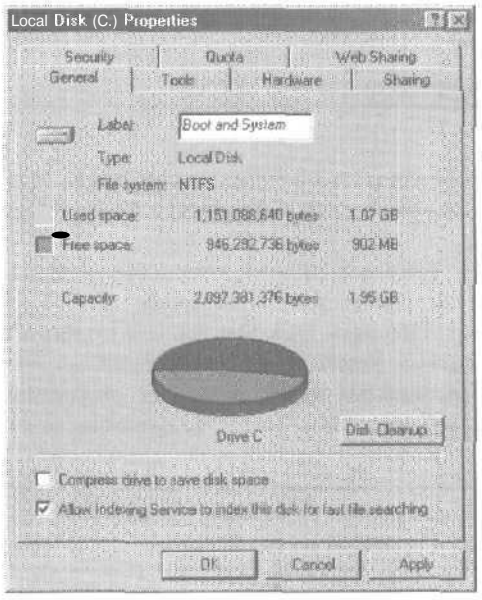


Рис. 4-6. Диалоговое окно свойств локального тома

В таблице описаны вкладки диалогового окна свойств тома.

Вкладка	Описание
Sharing (Доступ)	Служит для настройки параметров и разрешений общего тома в сети.
Hardware (Оборудование)	Служит для проверки свойств и разрешения конфликтов жестких дисков.

(окончание)

Вкладка	Описание
General (Общие)	Показывает метку и тип тома, файловую систему, занятое и свободное пространство. Если Вы хотите удалить ненужные файлы, щелкните кнопку Disk Cleanup (Очистка диска). Для томов NTFS можно установить два параметра: Compress drive to save disk space (Сжимать диск для экономии места) и Allow Indexing Service to index this drive for fast file searching (Разрешить индексирование диска для быстрого поиска).
Tools (Сервис)	Служит для проверки ошибок, архивирования и дефрагментации.
Web Sharing (Доступ через веб)	Служит для совместного использования папок через службу IIS (Internet Information Services). Вкладка появится, только если в Windows 2000 Server установлена служба IIS или в Windows 2000 Professional установлен Personal Web Server.
Security (Безопасность)	Служит для установки разрешений доступа в NTFS, доступна только для NTFS 4.0/5.0. (Windows 2000 использует NTFS 5.0.)
Quota (Квота)	Служит для квотирования томов NTFS 5.O.

Команды Refresh и Rescan

При работе с Disk Management может понадобиться обновить информацию на экране. Для этого в меню Action (Действие) предусмотрены команды Refresh (Обновить) и Rescan Disks (Повторить сканирование дисков).

Первая обновляет информацию о букве диска, файловой системе, томе и съемном носителе и определяет, можно ли прочитать тома, которые раньше не читались.

Вторая обновляет информацию об устройствах. При этом Disk Management сканирует все изменения в конфигурации подключенных дисков. Rescan Disks также обновляет информацию о съемном носителе, дисках CD-ROM, простых томах, файловых системах и буквах дисков. Сканирование дисков может занять несколько минут в зависимости от числа установленных устройств.

Примечание Чтобы выполнить команду Refresh или Rescan Disks, надо выбрать в оснастке Computer Management папку Disk Management или любой из ее объектов.

Обслуживание дисков удаленного компьютера

Если Вы входите в состав групп Administrators (Администраторы) или Server Operators (Операторы сервера), Вы можете обслуживать диски компьютеров с Windows 2000, которые входят в состав той же рабочей группы, домена или доверенного домена с любого другого компьютера сети под управлением Windows 2000.

Для удаленного обслуживания компьютера надо создать консоль MMC, связанную с этим компьютером. О консоли MMC см. главу 7.

Упражнение 1: настройка базового диска и его преобразование в динамический диск

Windows 2000 Server должен быть установлен, как описано в главе 2, Server01 должен содержать неразмеченное пространство, как указано в разделе «Об этой книге».

► Задание 1: установите FTP

Для выполнения задания 2 надо установить службу FTP Server на ServerOl. Об этой службе см. занятие 2 главы 14.

1. Вставьте компакт диск с Windows 2000 Server в дисковод CD-ROM.
2. Раскройте меню Start\Settings (Пуск\Настройка) и щелкните ярлык Control Panel.

   Откроется окно Control Panel (Панель управления).
3. Дважды щелкните значок Add/Remove Programs.

   Откроется одноименное окно.
4. Щелкните кнопку Add/Remove Windows Components (Установка и удаление компонентов Windows).

   Откроется окно мастера компонентов Windows.
5. В перечне компонентов выберите Internet Information Services (IIS) и щелкните кнопку Details (Состав).

   Откроется диалоговое окно Internet Information Services (US).
6. В перечне компонентов IIS пометьте флажок File Transfer Protocol (FTP) Server (FTP-сервер).
7. Щелкните кнопку OK.

   Откроется окно мастера компонентов Windows.
8. Щелкните кнопку Next (Далее).

   Откроется окно Configuring Components (Настройка компонентов) с индикатором внесения изменений в конфигурацию. Чуть позже откроется окно мастера Completeing the Windows Components Wizard (Завершение работы мастера компонентов Windows).
9. Щелкните кнопку Finish (Готово).

   Откроется окно Add/Remove Programs
10. Щелкните кнопку Close (Закрыть).
11. Закройте окно Control Panel.

► Задание 2: задействуйте оснастки Disk Management

Используя неразмеченное пространство диска 0 на ServerOl, создайте несколько основных разделов и один дополнительный. Чтобы выполнить задание, войдите в систему как Administrator (Администратор) с паролем password.

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Computer Management.

   Откроется окно оснастки Computer Management.
2. В дереве консоли раскройте узел Storage (Запоминающие устройства) и выберите Disk Management.

   На правой панели откроются окна с перечнем томов (сверху) и их графическим представлением (снизу). Диск 0 содержит основной раздел C:, а оставшееся пространство не размечено.
3. Щелкните неразмеченное пространство на графической панели.

4. В меню Action (Действие) выберите АЛ Tasks (Все задачи), а затем — команду Create Partition (Создать раздел).

   Откроется окно мастера создания раздела.

5. Ознакомьтесь с информацией в первом окне мастера и щелкните кнопку Next.
6. В окне Select Partition Type (Выберите тип раздела) щелкните переключатель Primary Partition (Основной раздел), а затем — Next.
7. В окне Specify Partition Size (Указание размера раздела) измените значение Amount Of Disk Space To Use (Размер создаваемого раздела) на 50 и щелкните кнопку Next.
8. В окне Assign Drive Letter Or Path (Назначение буквы диска или пути) в списке назначения буквы диска выберите H: и щелкните Next.
9. В окне Format Partition (Форматирование раздела) щелкните переключатель Format This Partition With The Following Settings (Форматировать данный раздел следующим образом), пометьте флажок Perform A Quick Format (Быстрое форматирование) и щелкните Next,
10. Просмотрите информацию в окне Completing The Create Partition Wizard (Завершение работы матера создания раздела) и щелкните кнопку Finish (Готово).

    Раздел H: появится в панели с графическим представлением содержания дисков.

11. Если появится сообщение System Change (Изменение параметров системы), щелкните кнопку Yes (Да), чтобы перезагрузить компьютер. После перезагрузки снова войдите в систему как Administrator с паролем password.
12. Выполнив предыдущие этапы этого задания, создайте из оставшегося неразмеченного пространства диска 0 конфигурацию на основе данных таблицы.

Пип раздела	Размер (Мб)	Диск	Формат
Основной	100	I	FAT32
Дополнительный	Оставшееся неразмеченное пространство	Нет	Нет

13. Просмотрите свойства дисков H: и I: в перечне томов. Свободное пространство в графической панели не содержит букв дисков. Эта область является дополнительным разделом и используется для создания логических дисков.
14. В графической панели щелкните свободное пространство дополнительного раздела,
15. В меню Action выберите All Tasks, а затем — Create Logical Drive (Создать логический диск).

    Откроется окно мастера создания раздела.

16. Ознакомившись с информацией в первом окне, щелкните Next.
17. В окне Select Partition Type (Выберите тип раздела) щелкните переключатель Logical Drive (Логический диск), а затем — Next.
18. В окне Specify Partition Size (Указание размера раздела) измените значение Amount Of Disk Space To Use (Размер создаваемого раздела) на 150 и щелкните Next.
19. В окне Assign Drive Letter or Path (Назначение буквы диска или пути) щелкните переключатель Mount This Volume At An Empty Folder That Supports Drive Paths (Подключить том как пустую папку, поддерживающую путь), а затем — кнопку Browse (Обзор).

    Откроется окно Browse For Drive Path (Поиск пути к диску).

20. Раскройте диск C:\, а затем — каталог Inetpub.
21. Щелкните подкаталог ftproot, а затем — кнопку OK.

    В переключателе Mount This Volume At An Empty Folder That Supports Drive Paths будет указан путь C:\Inetpub\ftproot.

22. Щелкните кнопку Next (Далее).

23. В окне Format Partition (Форматирование раздела) выберите быстрое форматирование раздела под **NTFS,** измените метку тома на *FTPVol* и отмените сжатие файлов и папок.
24. Щелкните Next.
25. Просмотрев сводную информацию в окне Completing The Create Partition Wizard (Завершение работы матера создания раздела), щелкните кнопку Finish (Готово).

    Так как Вы не указали имена томов, вместо H: и I: используются соответственно имена NEW VOLUME (H:) и NEW VOLUME (I:).
26. Чтобы изменить имена томов, в перечне томов или на графической панели щелкните NEW VOLUME (H:) [Новый том (H:)].
27. В меню Action выберите All Tasks, а затем — Properties.

    Откроется диалоговое окно New Volume (H:) Properties [Свойства: Новый том (H:)].
28. Удалите строку New Volume (Новый том) в поле Label (Метка) и щелкните OK.
29. Повторите последние три пп. для тома NEW VOLUME (I:).

    В результате Вы получите следующую конфигурацию диска 0:

Диск/Путь	Формат	Тип	Предназначение
C:	NTFS	Основной	Системный (а также загрузочный раздел, хотя он не показан в оснастке Disk Management).
H:	NTFS	Основной	Не используется.
I:	FAT32	Основной	Не используется.
C:\Inetpub\ ftproot	NTFS	Дополнительный	Файлы, сохраняемые в c:\Inetpub\ftproot, перенаправляются на этот раздел диска.
Нет	Нет	Дополнительный	Свободное пространство. (Его размер зависит от размера диска 0.)

30. Проверьте, что том FTPVol доступен через C:\Inetpub\ftproot. Для этого откройте Windows Explorer (Проводник).
31. В дереве консоли раскройте My Computer (Мой компьютер), а затем — папку C:\Inetpub.

    Палка ftproot имеет значок диска. Все файлы, хранящиеся в C:\Inetpub\ftproot, перенаправляются на том FTPVol дополнительного раздела.
32. Закройте Windows Explorer, а затем и оснастку Computer Management.

Резюме

Чтобы подготовить к работе жесткий диск, надо указать его тип, разбить его на разделы и отформатировать. Windows 2000 поддерживает два типа дисков: базовые и динамические. Базовые диски могут содержать основные и дополнительный разделы и логические диски на дополнительном разделе. По умолчанию в Windows 2000 используется базовая структура дисков, поэтому все диски являются базовыми, пока их не преобразуют в динамические. Динамические диски содержат один раздел, охватывающий весь диск. Динамический диск можно разделить на тома, способные включать пространство одного или нескольких физических дисков. Оснастка Disk Management позволяет просмотреть сведения об имеющихся дисках, а также обслуживать диски, например, создавать и удалять разделы и тома. Имея соответствующие права, Вы можете обслуживать диски локально или с удаленного компьютера: кроме мониторинга информации о дисках, Вы сможете добавлять, удалять и изменять их тип.

Занятие 2. Файловая система FAT

Windows 2000 поддерживает две версии FAT: FAT16 и FAT32.

Изучив материал этого занятия, Вы сможете:

✓ описать реализацию FAT16 и FAT32 в Windows 2000.

Продолжительность занятия - около 25 минут.

Введение

Файловая система FAT была создана еще тогда, когда размер дисков был мал, а структура каталогов очень проста. Для зашиты файловой системы на томе находятся две копии таблицы расположения файлов, и в случае разрушения одной копии таблицы используется другая. Для загрузки системы таблица FAT должна храниться в точно определенном месте на диске.

FAT16 работает в Windows 2000 так же, как в MS-DOS, Windows 3.x/95/98, а FAT32 - как в Windows 95 OSR2/98. Windows 2000 можно установить на существующий основной раздел FAT или логический диск. В Windows 2000 можно перемешать или копировать файлы между томами FAT и NTFS.

Windows 2000 нельзя использовать совместно с программами сжатия или разбиения на разделы, которым требуется доступ к дискам средствами MS-DOS. Поэтому такие программы, как MS-DOS 6.0 DoubleSpace или MS-DOS 6.22 DiskSpace, нельзя активизировать на основных разделах FAT или логических дисках, к которым надо иметь доступ в Windows 2000.

Файловая система FAT16

Диск в файловой системе FAT состоит из секторов по 512 байт. Сектор — это наименьшая единица, используемая при чтении/записи данных.

Наименьшей единицей, которую ОС использует для размещения файла в разделе FAT, является кластер; Размер кластера зависит от размера раздела и может достигать 64 кб.

Каждый кластер **раздела в таблице FAT, определяется как:**

- неиспользуемый;
- используемый файлом;
- испорченный;
- **последний** кластер **файла.**

Примечание Тома объемом менее 16 Мб обычно будут форматироваться под 12-разрядную FAT, но точный размер зависит от конфигурации диска. FAT12 — первая версия файловой системы FAT, предназначенная для очень маленьких носителей. Используя меньший размер записей, FAT экономит дисковое пространство. Поэтому в FAT12 объем доступного пространства больше, чем в остальных файловых системах. Сейчас FAT12 можно встретить только на очень малых или старых носителях. Например, 3,5-дюймовые носители используют FAT16, а 5,25-дюймовые — FAT12.

На рис. 4-7 представлена структура тома FAT16. Корневой каталог содержит записи для всех файлов и папок тома. Единственное отличие корневой папки от остальных папок в том, что она находится в точно определенной области диска и содержит записи фиксированного размера по 512 байт. Количество записей гибкого диска зависит от его размера.

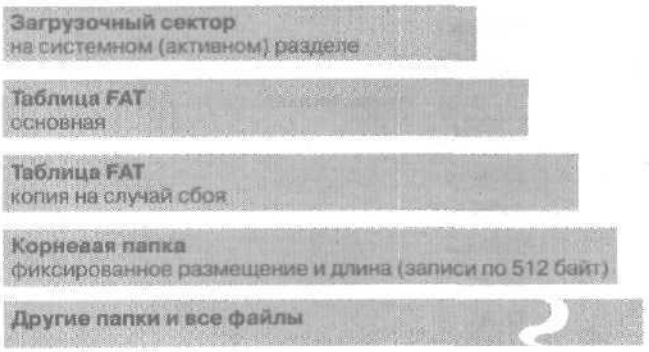


Рис. 4-7, Структура тома FAT16

Папки хранят записи для каждого файла и подпапки. Их атрибуты таковы:

Атрибуты записи	Количествобит
Имя	Формат 8.3
Атрибут	8
Время создания	24
Дата создания	16
Дата последнего доступа	16
Время последнего изменения	16
Дата последнего изменения	16
Начальный кластер в FAT	16
Размер файла	32

Структура папок FAT организации не имеет — файлы записываются в первое доступное место тома. Начальный кластер представляет собой адрес первого кластера, используемого файлом. Каждый кластер содержит указатель на следующий кластер файла или шестнадцатеричный признак конца файла (OxFFFF).

Информацию в папке может использовать любая ОС, поддерживающая FAT. Windows NT хранит дополнительные временные метки в записи папки FAT. Эти метки содержат время создания или последнего доступа к файлу; к ним преимущественно обращаются POSIX-приложения.

Все записи в папке имеют одинаковый размер, а значит, о том, что представляет собой та или иная запись, можно узнать по байту атрибута. Например, один бит указывает, что запись предназначена для подпапки, а другой — что она является меткой тома. Обычно установку этих битов контролирует только ОС.

Пользователь может устанавливать 4 бита из байта атрибута:

- архивный файл;
- системный файл;
- скрытый файл;
- файл только для чтения.

FAT16 включена в Windows 2000 для совместимости с предыдущими версиями Windows и другими ОС.

Как и в предыдущих версиях, в Windows 2000 размер раздела FAT16 ограничен 4 Гб. Стандартный размер кластера определяется размером раздела. Стандартные размеры кластеров для томов FAT16 таковы:

Размер раздела	Количество секторов в кластере	Размер кластера
0–32 Мб	1	512 байт (эквивалентен размеру сектора раздела)
33–64 Мб	2	1 024 байт
65–128 Мб	4	2 048 байт
129-256 Мб	8	4 096 байт
256–512 Мб	16	8192 байт
512–1 024 Мб	32	16 Кб
1 024-2 048 Мб	64	32 кб
2 048-4 096 Мб	128	64 кб

При форматировании раздела утилитой Format можно указать другой размер кластеров, задав параметр /a:*размер*, однако настоятельно рекомендуется использовать стандартные значения.

Примечание Диски, поддерживающие секторы размером более 512 байт, могут использовать кластеры размером 128 и 256 кб. Впрочем, чем больше размер кластера, тем больше пространства теряется. Большой размер кластера годится для хранения очень объемных файлов, например баз данных.

Файловая система FAT32

Основным преимуществом FAT32 над FAT16 является поддержка разделов большего объема. FAT16 поддерживает разделы до 4 Гб, а FAT32 — до 2 047 Гб. В Windows 2000 размер создаваемого тома ограничен 32 Гб, но можно смонтировать тома и большего размера. Исключая это ограничение форматирования дисков, возможности и формат FAT32 в Windows 2000 аналогичны их реализации в Windows 95 OSR2/98.

Для совместимости с существующими программами, сетями и драйверами устройств FAT32 спроектирована с минимальными отклонениями от архитектуры, внутренних структур данных, API-интерфейсов и формата FAT16.

Так как сейчас для хранения значений кластеров требуется 4 байта, многие внутренние и дисковые структуры данных и API-интерфейсы исправлены и расширены. Некоторые API-интерфейсы более не применяются во избежание повреждения диска старыми утилитами. Эти изменения не отразятся на работе большинства программ. Существующие утилиты и драйверы FAT должны нормально работать с разделами FAT32. Дисковые утилиты для MS-DOS надо обновить, чтобы они могли поддерживать драйверы FAT32.

Структура разделов FAT32

Файловая система FAT32 преодолела барьер в 4 Гб, ограничивавший объем разделов. Форматируя разделы размером 4 Гб и более под FAT16, надо использовать кластеры размером не менее 32 кб.

Максимальный размер файла в FAT32 — 4 Гб — 2 байта. FAT32 использует для таблицы расположения файлов 4 байта каждого кластера, а FAT16 — 2 байта.

Раздел FAT32 должен содержать не менее 65 527 кластеров, и их размер увеличить нельзя. На рис. 4-8 изображена структура раздела FAT32.

Файловые системы FAT16 и FAT32 плохо масштабируемы. При увеличении размера тома растет таблица расположения файлов. Один из недостатков большой таблицы FAT – увеличение времени, требуемое ОС для определения объема свободного объема загрузочного тома после перезагрузки.

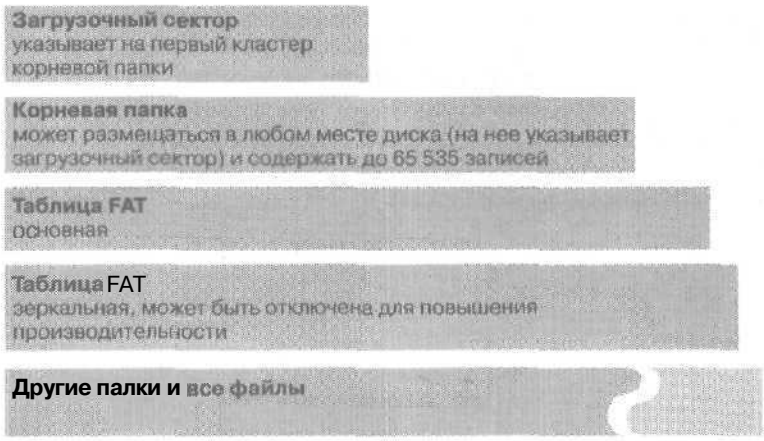


Рис. 4-8. Структура тома FAT32

Таблица расположения файлов представляет собой упакованный список 32-разрядных записей, связанных один в один с кластерами. Структура папок организована в FAT32 так же, как и длинные имена файлов в Windows 95. Единственное отличие заключается в добавлении поля верхнего слова для кластера в записях каталогов, ссылающихся на номера кластеров.

Ограничения FAT32

Максимальный размер тома в FAT32 ограничен максимальным числом записей FAT, числом секторов в кластере и 32-разрядным числом секторов в записи раздела. (Предполагается, что размер сектора составляет 512 байт.)

Таблица связывает максимальный размер раздела с размером кластеров:

Размер кластера	Максимальный размер тома
512 байт	127,9 Гб
1 кб	255,9 Гб
2 кб	511,9 Гб
4 кб	1 023,9 Гб или 1 Терабайт (Тб)
8 кб	2 047 Гб (2 Тб)
16 кб	2 047 Гб (2 Тб)
32 кб	2 047 Гб (2 Тб)

Помните: размер создаваемого тома в Windows 2000 не может превышать 32 Гб, но разрешается монтировать тома большего размера, созданные в другой ОС, например в Windows 98.

Резюме

Файловая система FAT спроектирована для небольших дисков и простой структуры папок. Windows 2000 поддерживает две версии файловой системы FAT: FAT16 и FAT32. Раздел FAT16 делится на секторы по 512 байт. Для записи файлов на диск применяются кластеры. Стандартный размер кластера определяется размером раздела и может иметь объем от 4 (8 секторов) до 64 (128 секторов) кб. Основное преимущество FAT32 над FAT16 — поддержка разделов большего объема. FAT16 поддерживает разделы размером до 4 Гб, FAT32 — до 2 047 Гб, В Windows 2000 размер создаваемого тома не может превышать 32 Гб, хотя можно монтировать тома размером больше 32 Гб, созданные в других ОС. FAT32 спроектирована с минимальными отклонениями от архитектуры, внутренних структур данных, API-интерфейсов и дискового формата FAT16.

Занятие 3. Файловая система NTFS

Windows 2000 поддерживает последнюю, пятую версию NTFS, которая обладает более высокими скоростными характеристиками, надежностью и совместимостью по сравнению с FAT. Структуры данных NTFS позволяют реализовать такие возможности Windows 2000, как службы Active Directory, программы управления и хранилища, основанные на точках переопределения. NTFS включает функции защиты, необходимые для корпоративных файл-серверов и высококлассных персональных компьютеров, а также поддерживает контроль и разрешения доступа к данным, необходимые для обеспечения их целостности.

Изучив материал этого занятия, Вы сможете:

- ✓ описать реализацию NTFS в Windows 2000.

Продолжительность занятия — около 45 минут.

Введение в NTFS

Microsoft рекомендует форматировать все разделы Windows 2000 под NTFS, исключая конфигурации с альтернативной загрузкой, при которых используются другие ОС (не Windows 2000/NT). Форматирование разделов Windows 2000 под NTFS вместо FAT позволяет задействовать возможности, доступные только в NTFS, включая восстановление после сбоя и сжатие. Для восстановления после сбоев в NTFS реализовано так, что пользователь должен время от времени запускать программу проверки диска, NTFS обеспечивает целостность тома за счет стандартных технологий восстановления, применяющих журнал транзакций. Кроме того, Windows 2000 на основе разделов NTFS поддерживает сжатие на уровне каталогов и отдельных файлов. Сжатые таким образом файлы могут читаться и записываться любыми приложениями без предварительной распаковки отдельной программой.

NTFS поддерживает все возможности Windows 2000, имеет более высокую скорость доступа, чем FAT, и минимизирует число обращений к диску, необходимых для поиска файла. NTFS позволяет также назначать разрешения на уровне файлов и каталогов. Разрешения, назначаемые для файлов и папок в NTFS, распространяются не только на пользователей, работающих на компьютере, где хранится файл, но и работающих в сети и обращающихся к общему ресурсу. Кроме того, можно комбинировать разрешения доступа к общим папкам и разрешения NTFS, FAT поддерживает разрешения доступа только к общим папкам из сети.

Совет Не устанавливайте разрешения доступа к общим папкам для разделов NTFS — используйте локальные разрешения NTFS.

Возможности Windows 2000

NTFS поддерживает все новые функции и усовершенствования Windows 2000.

Точки переопределения

Тонки переопределения (reparse points) — это новые объекты NTFS в Windows 2000. Точка переопределения — это файл или каталог, содержащий контролируемые пользователем данные в администрируемом системой *атрибуте переопределения* (reparse attribute). Фильтры файловой системы используют его для изменения обычного поведения ОС при обра-

щении к файлам и каталогам, Таким образом, скорость работы с файлом/каталогом, содержащими точку переопределения в NTFS, выше, чем с обычными файлами/каталогами в других файловых системах.

Точки переопределения позволяют файловой системе изменить механизм обработки запроса файла или папки. В итоге процесс обработки доступа к файлу повторно инициируется с новым, контролируемым пользователем контекстом. Если точка переопределения содержит закрытые данные переопределения, доступ к ним открывается всем фильтрам файловой системы через соответствующий буфер.

Для различения точек переопределения применяются *теги переопределения* (reparse tags). Если при анализе пути к файлу встречается объект файловой системы с атрибутом переопределения, он передается обратно в стек драйвера файловой системы для модификации механизма ввода-вывода. Переопределение ввода-вывода, обрабатываемое фильтрами файловой системы, включает идентификацию тегов переопределения. Каждый драйвер выполняет специфические действия системы ввода-вывода и использует теги и *глобальные уникальные идентификаторы* (globally unique identifiers, GUID), чтобы распознать вызовы системы ввода-вывода, за которые они отвечают. Хотя сами теги переопределения уникальны, GUID обеспечивают дополнительную идентификацию.

При обращении пользователя к каталогу, содержащему связанный с ней атрибут переопределения, происходит следующее.

1. Пользователь открывает Windows Explorer (Проводник) и дважды щелкает папку в томе NTFS.
2. Вызов переводится из пользовательского режима в режим ядра, где достигает системного объекта файла и обнаруживает соответствующий атрибут переопределения.
3. Любой фильтр файловой системы, установленный в Windows 2000, проверяет стек ввода-вывода на наличие тегов, ассоциированных с точкой переопределения. Обнаружив совпадение, фильтр прерывает вызов. Фильтры файловой системы проверяют как входящие, так и исходящие вызовы.
4. Прервав вызов, фильтр, отвечающий за совпадение имен каталогов, выполняет дополнительные действия, связанные с точкой переопределения. При совпадении имен каталогов драйвер монтирует дополнительное пространство имен.
5. Драйвер файловой системы возвращает вызов в приложение, монтирует дополнительное пространство имен и возвращает управление генерировавшей вызов функции.

Примечание Если точка переопределения обнаружена не будет, запрос к открытому каталогу не будет перехвачен драйвером фильтра файловой системы в стеке ввода-вывода, и будет задействован стандартный механизм обработки запроса каталога.

Windows 2000 позволяет изменить относительный порядок файловых систем в стеке. На основе информации в реестре можно поместить фильтр над или под любым другим фильтром. NTFS всегда помещается под фильтрами файловой системы, которые обращаются к NTFS как к службе, и над драйверами устройств, используемыми самой NTFS,

Чтобы обслужить запросы служб и распределить очередность вызовов уровней, подсистема ввода-вывода Windows 2000 строит соответствующие структуры данных. После обработки функции стеком подсистема ввода-вывода проверяет результат операции и либо выдает следующие рабочие запросы, либо сбрасывает нормально завершившиеся запросы.

Точки переопределения лежат в основе двух усовершенствований NTFS.

- Управление иерархическими запоминающими устройствами. Неиспользуемые файлы автоматически архивируются на более дешевое устройство, например, пленку или съемный диск. При попытке доступа к архивному файлу ОС с помощью точки переопреде-

ления находит его на альтернативном устройстве. Для пользователя этот процесс прозрачен, и файл не является архивным.

- Точка монтирования тома позволяет отображать несколько томов как один диск.

Естественное структурированное хранилище

Новинка Windows 2000 — естественное структурированное хранилище (Native Structured Storage, NSS) — позволяет хранить документы ActiveX в том же многопоточном формате, который технология ActiveX применяет для логической обработки структурированного хранилища. Фильтр NSS для файловой системы представляет файл на диске как OLE-структурированное хранилище файлов. В результате повышается эффективность физического хранения документов ActiveX. Данные каждого внедренного объекта теперь хранятся в собственном потоке внутри одного файла. При обновлении объекта для него создается новый поток, старый уничтожается, и на диске освобождается место. Фильтр NSS выполняет все эти операции прозрачно для приложения, позволяя копировать NSS-файлы на дискету и преобразовывать их в обычный формат и обратно.

Любой файл, использующий NSS, должен содержать точку переопределения, которая указывает:

- что файл состоит из нескольких потоков;
- файловой системе преобразовать несколько потоков в один при использовании файла в системе, не поддерживающей NSS.

Квотирование дисков

В Windows 2000 можно ограничивать размер дискового пространства сервера, к которому обращается пользователь. Утилита Disk Quotas (Дисковые квоты) позволяет администратору управлять ростом хранилищ в распределенных средах. Квотирование дисков в NTFS для Windows 2000 применяется к каждому разделу по отдельности (см. главу 13).

Поддержка разреженных файлов

Разреженные файлы (sparse files) позволяют программам создавать очень большие файлы, но хранить их на минимуме дискового пространства. NTFS обрабатывает потоки разреженных данных так, что фактически на диске размещаются только значимые данные. Когда программа запрашивает разреженный файл, файловая система извлекает значимые данные, а избыточные заменяет нулями.

Для работы с разреженными файлами надо задать соответствующий атрибут файловой системы. После этого она эффективно задействует возможности разреженных файлов, сохраняя на диске только значимые данные. API-интерфейсы файловой системы позволяют копировать и архивировать файлы как в исходном, так и в разреженном виде. В итоге поддержка разреженных файлов повышает эффективность использования дискового пространства и производительность.

Атрибут разреженного файла заставляет подсистему ввода-вывода воспринимать только значимые данные. Фактически на диске размещаются только значимые (ненулевые) данные, а незначащие (большие строки данных, состоящие из нулей) — нет. Согласно требованиям спецификации безопасности C2 при чтении разреженного файла избыточные данные заменяются нулями.

Использование разреженных файлов

NTFS поддерживает разреженные файлы как в сжатом, так и несжатом виде. NTFS обрабатывает операции чтения разреженных файлов, возвращая значимые и незначимые данные на основе карты файла. Допускается чтение разреженного файла без извлечения

всего объема его данных. Это удобная функция для приложений, которым надо эффективно обрабатывать крупные файлы. По умолчанию NTFS возвращает весь набор данных файла.

Разреженные потоки данных характеризуются двумя параметрами: AllocatedLength округляется до размера в кластерах, превышает или равен размеру потока, а TotalAllocatedLength представляет фактическое количество кластеров, выделенных потоку. Значение TotalAllocatedLength всегда меньше или равно значению AllocatedLength.

Рассмотрим научное приложение, использующее матрицу размером 1Тб. Значимые данные в ней занимают только 1Мб. Если установлен атрибут разреженного файла, файловая система вместо хранения на диске всех данных размещает только значимые. Когда программа запрашивает разреженный файл, файловая система извлекает размещенные значимые данные, а избыточные заменяет нулями. В итоге дисковое пространство будет использоваться эффективно, а при обращении к файлу будет возвращаться корректная последовательность битов.

Проверка ссылок и идентификаторы объектов

Windows 2000 позволяет приложениям отслеживать ссылки на ресурсы, перенесенные локально или внутри домена. Подписавшись на эту службу, клиенты сохраняют целостность ссылок. *Проверка ссылок* (link tracking) хранит уникальные идентификаторы объектов, что позволяет автоматически изменить путь для ярлыков к перемещенному файлу или папке.

Служба проверки ссылок отслеживает ресурсы, перемещенные между томами NTFS 5.0 локально или внутри одного домена. Она может отследить изменение сетевого имени машины, сетевого имени общей папки или перемещение тома на другую машину.

Журнал изменений

Представляет собой разреженный поток, регистрирующий сведения о добавлении, удалении и изменении каждого тома NTFS. *Журнал изменений* (change journal) предназначен для приложений — индексов файловой системы, диспетчеров репликации, удаленных хранилищ и архиваторов, которым надо знать, что происходит на определенном томе.

С журналом изменений только небольшой активный диапазон файла использует пространство на диске. Активный диапазон обычно начинается с нулевого смещения в потоке. Реальное смещение в потоке представляет *уникальный порядковый номер* (Unique Sequence Number, USN) конкретной записи обновления. По мере перемещения активного диапазона по потоку предыдущие записи освобождаются и становятся недоступными. Размер активного диапазона разреженного файла можно настроить.

Для определения изменений в пространстве имен журнал USN эффективнее регистрации штампов времени или модификаций файлов. Системный администратор может просмотреть изменения, случившиеся на томе, не изучая текущего состояния пространства имен.

Журнал изменений не влияет на работу приложений, если они не спроектированы для его использования. Он работает в связанном пространстве имен, основываясь на потоке разреженных данных, что позволяет освобождать место в начале разреженного файла. В результате записи изменений могут исчезнуть, и приложения, которым они требуются, должны быть готовы к такому повороту событий. Журнал изменений хранит записи для каждого тома, отформатированного под NTFS 5.O.

Уникальный порядковый номер обновления

В журнале USN регистрируются все изменения, выполненные над файлом тома. Таким образом приложения узнают об изменениях наборов файлов. Журнал USN эффективнее проверки штампов времени или регистрация изменений файла.

Когда пользователь, администратор или другой контроллер домена обновляет объект в каталоге, контроллер этого объекта назначает операции изменения USN. Каждый контроллер обслуживает собственный список USN и вносит изменения в каталог последовательно, согласно их номерам. Каждый контроллер домена ведет также таблицу USN, полученных от остальных контроллеров домена.

Фиксируя изменение в каталоге, контроллер домена записывает и USN-изменения. Это атомарная операция, поэтому контроллер либо регистрирует изменение свойства и USN-модификации, либо не вносит никаких изменений.

Поддержка CD и DVD

Windows 2000 поддерживает файловые системы CDFS и UDF и устройства DVD.

Файловая система CD-ROM

Windows 2000 поддерживает файловую систему только для чтения CDFS, совместимую со стандартом ISO 9660, и длинные имена файлов согласно ISO 9660 уровня 2.

Используя CD-ROM в Windows 2000, учтите, что:

- имена файлов и каталогов должны быть короче 32 символов;
- имена файлов и каталогов должны состоять из заглавных букв;
- количество уровней дерева каталогов не должно превышать 8;
- расширения файлов не обязательны.

Примечание CDFS не поддерживает строчных букв в имени файла. При указании имени файла или каталога на CD-ROM строчными буквами появится сообщение, что файл не найден.

Файловая система UDF

Новая файловая система Windows 2000 UDF создана для обмена данными между DVD и CD. Основная цель UDF — поддержка устройств только для чтения DVD-ROM. Файловая система UDF основана на стандарте ISO 13346.

В таблице описаны требования и ограничения UDF:

Элемент	Требования
Размер логического/физического сектора	Размеры логического и физического сектора тома должны совпадать.
Размерлогическогоблока	Размер логического блока логического тома должен быть равен размеру логического сектора тома.
Размерфизическогосектора набора томов	Размеры физических секторов всех носителей одного набора томов должны совпадать.

В UDF поддержка нескольких томов и нескольких разделов не обязательна. Поддерживаются только носители дозаписи, перезаписи и WORM. Windows 2000 самостоятельно поддерживает только формат для чтения UDF. Возможности дозаписи, перезаписи и WORM должны поддерживаться приложениями сторонних фирм.

Поддержка DVD

Объем диска DVD превышает объем обычного CD примерно в 20 раз, что позволяет хранить большие объемы видео- и звуковых данных. Поддержка DVD в Windows — это не только внедрение нового драйвера. DVD сочетает широкий спектр возможностей и технологий, поэтому устройство чтения DVD-дисков следует рассматривать в контексте всего

компьютера. Устройства и диски DVD-ROM наиболее эффективны для хранения больших файлов с точки зрения их стоимости. Скоро появятся устройства записи DVD, которые еще больше расширят спектр применений этой технологии.

Примечание Библиотека Microsoft Solution Developer Network (MSDN) теперь доступна на DVD-ROM.

На компьютерах с поддержкой DVD устройство будет работать как обычный диск, а при наличии оборудования декодирования Вы сможете насладиться и полноценным воспроизведением DVD.

Некоторые компоненты системы изменятся на основе таких достижений, как, например, Accelerated Graphics Port (AGP) или улучшенная шина PCI. Однако неизменно будут присутствовать драйвер DVD-ROM, файловая система UDF, драйвер потокового класса WDM и разветвитель-навигатор DVD.

Драйвер класса DVD-ROM

DVD-ROM имеет собственный встроенный набор команд. В Windows 98 их поддержку обеспечивал обновленный драйвер класса CD-ROM. В Windows 2000 появился новый драйвер устройства WDM DVD-ROM, обеспечивающий чтение секторов на диске DVD-ROM.

Поддержка UDF нужна для совместимости с DVD-дисками, отформатированными под UDF. Windows 2000 поддерживает файловую систему UDF, устанавливаемую аналогично FAT16 и FAT32.

Защита авторских прав

Зашита авторских прав для DVD осушествляется путем шифрования важных секторов диска и последующей расшифровки непосредственно перед чтением данных. Microsoft будет обеспечивать поддержку аппаратных и программных дешифраторов с помощью программных модулей, отвечающих за аутентификацию между декодером и драйвером DVD-ROM.

Региональные ***ограничения***

В рамках программы зашиты авторских прав содержимого DVD-дисков земной шар был разбит на шесть регионов. Указывая код региона, автор содержания диска определяет, где будет разрешено воспроизводить DVD-диск. Microsoft будет производить ПО, отвечающее за обработку региональных кодов, назначенных консорциумом DVD.

Структура NTFS

В этом разделе обсуждаются основные компоненты файловой системы NTFS: структура томов NTFS, загрузочный сектор Windows 2000, таблица Master File Table, метаданные и атрибуты файлов в NTFS.

Структура тома NTFS

В качестве фундаментальной единицы размещения информации NTFS использует кластеры, состоящие из одного или нескольких секторов. Стандартный размер кластеров зависит от размера раздела. Из оснастки Disk Management пользователь может указать свой размер кластеров до 4 кб (4 096 байт). Если для форматирования тома NTFS применяется программа Format.exe, пользователь может задать любой стандартный размер кластера.

Внимание! NTFS не поддерживает сжатие для кластеров размером более 4 кб.

В таблице перечислены рекомендуемые размеры кластеров. Размер кластеров можно изменить, однако для этого придется переформатировать раздел.

Размер раздела	Количество секторов в кластере	Размер кластера
до 512 Мб	1	512 байт
513–1 024 Мб	2	1 кб
1 025-2 048 Мб	4	2 кб
2 049-4 096 Мб	8	4 кб
4 097-8 192 Мб	16	8 кб
8 193-16 384 Мб	32	16 кб
16 385–32 768 Мб	64	32 кб
> 32 768 Мб	128	64 кб

Загрузочный сектор Windows 2000

Любой том NTFS содержит загрузочный сектор. Загрузочный сектор начинается с нулевого сектора и занимает до 16 секторов. Он состоит из двух частей:

- блок параметров BIOS содержит сведения о структуре тома и структурах файловой системы;
- код, описывающий, как найти системные файлы для загрузки ОС; в Windows 2000 на компьютерах с *x*86-процессорами этот код загружает файл Ntldr.

Таблица MFT и метаданные в Windows 2000

При форматировании тома под NTFS создаются таблица MFT (Master File Table) и метаданные. NTFS использует записи таблицы MFT для описания соответствующих им файлов. Записи MFT или внешнее хранилище, на которое ссылаются записи MFT, хранят всю информацию о файле, включая его размер, дату и время создания, права доступа и его содержимое.

Для каждого каталога и файла на томе NTFS в таблице MFT создается соответствующая запись. MFT также содержит отдельную запись о самой MFT. NTFS выделяет пространство под запись MFT в зависимости от размера кластеров файла. Атрибуты файла записываются в выделенное в таблице MFT пространство. Кроме атрибутов файла, каждая запись содержит данные о расположении записи файла в таблице M FT.

Обычно каждый файл занимает одну запись. Если же файл имеет большое количество атрибутов или сильно фрагментирован, может понадобиться больше записей. В этом случае первая запись файла (базовая) содержит ссылку на следующую. Небольшой файл (до 1 500 байт) целиком хранится в записи MFT.

Метаданные представляют собой файлы, которые NTFS использует для реализации структуры файловой системы. NTFS резервирует для метаданных первые 16 записей (около 1 Мб) в таблице MFT. Остальные записи таблицы описывают файлы и каталоги.

При искажении первой записи MFT файловая система считывает вторую запись, чтобы найти дубликат файла MFT. Сегмент данных для $Mft и $MftMjrr расположен на загрузочном секторе, дубликат которого находится в конце раздела.

Атрибуты файлов в NTFS

Каждый занятый сектор тома NTFS принадлежит файлу. Даже метаданные файловой системы являются частью файла. NTFS рассматривает каждый файл или каталог как набор атрибутов. Атрибутами являются такие элементы, как имя, информация о защите и даже содержимое файла.

Каждый атрибут определяется типом, кодом и именем атрибута. Если атрибуты файла вмешаются в его MFT-запись, они называются *резидентными* (resident attribute). Такими атрибутами всегда являются имя файла и его временные характеристики. Если информация о файле слишком велика, чтобы поместиться в MFT-записи, некоторые атрибуты становятся нерезидентными, Они занимают один или несколько кластеров в другом месте тома. Чтобы описать расположение всех записей атрибутов, NTFS создает атрибут Attribute List.

Использование NTFS

При использовании NTFS надо принимать во внимание несколько фактов: обновление до Windows 2000, альтернативную загрузку Windows 2000 и вопросы совместимости NTFS.

Обновление до Windows 2000

Обновление Windows NT до Windows 2000 (если нет альтернативной загрузки) может сказаться следующим образом;

- тома, отформатированные под раннюю версию NTFS, преобразуются в NTFS 5.0;
- загрузочные/системные тома, отформатированные под FAT16, преобразуются в NTFS 5.0;
- остальные тома не преобразуются.

Windows NT 4.0 Service Pack 4

При установке Windows 2000 на компьютер Windows NT 4.0 с установленным четвертым пакетом исправлений или более поздним при первой загрузке ОС тома NTFS автоматически обновляются до версии 5.0, а затем устанавливается новый драйвер NTFS для работы с этими томами.

Преобразование томов FAT

Тома FAT преобразуются в NTFS 5.0 только с согласия пользователя. Winnt32.exe, запущенная в автоматическом режиме, отобразит меню преобразования файловой системы, чтобы пользователь мог преобразовать разделы FAT в NTFS. Winnt32.exe, запущенная в неавтоматическом режиме, преобразует или оставит нетронутыми файловые системы в зависимости от значения параметра FileSystem в файле ответа. Преобразование будет выполнено автоматически, если FileSystem = ConvertNTFS, и не будет выполнено, если FileSystem = LeaveAlone. При установке Windows 2000 Server параметр преобразования FAT в NTFS будет включен. Если параметр FileSystem не указан, преобразование не выполняется.

Запустив установку с помощью Winnt.exe, загрузочного диска или CD-ROM, можно выбрать файловую систему в текстовом режиме установки.

Ниже представлена информация о переходе от FAT к NTFS.

Операционная система	От FAT к NTFS	От NTFS к NTFS 5.0
Windows NT 4.0 Workstation (SP4 и выше)	По умолчанию мастер предлагает не преобразовывать тома.	Все тома NTFS модернизируются до NTFS 5.О.
Windows NT 3.51 Workstation	По умолчанию мастер предлагает не преобразовывать тома.	Все тома NTFS модернизируются до NTFS 5.О. Появится предупреждение, и пользователь сможет продолжить или завершить настройку.

(окончание)

Операционная система	От FAT к NTFS	От NTFS к NTFS 5.0
Windows NT 3,51 Server (изолированный/ контроллер домена)	По умолчанию мастер предлагает преобразовать тома.	Все тома NTFS модернизируются до NTFS 5.O. Появится предупреждение, и пользователь сможет продолжить или завершить настройку,
Windows NT 4.0 Workstation (до SP3)	По умолчанию мастер предлагает не преобразовывать тома.	Все тома NTFS модернизируются до NTFS 5.O. Появится предупреждение, и пользователь сможет продолжить или завершить настройку.
Windows NT 4.0 Workstation (SP3)	По умолчанию мастер предлагает не преобразовывать тома.	Все тома NTFS модернизируются до NTFS 5.O. Появится предупреждение, и пользователь сможет продолжить или завершить настройку.
Windows NT 4.0 Server (до SP3 — изолированный /контроллер домена)	По умолчанию мастер предлагает преобразовать тома.	Все тома NTFS модернизируются до NTFS 5.O. Появится предупреждение, и пользователь сможет продолжить или завершить настройку.
Windows NT 4.0 Server (SP3 — изолированный/ контроллер домена)	По умолчанию мастер предлагает преобразовать тома.	Все тома NTFS модернизируются до NTFS 5.O.
Windows NT 4.0 Server [SP4 и выше — изолированный/контроллер домена)	По умолчанию мастер предлагает преобразовать тома.	Все тома NTFS модернизируются до NTFS 5.O.
Windows 95	Преобразование не выполняется. Файловая система остается прежней.	Нет
Windows 95 OSR2	Преобразование не выполняется. Файловая система остается прежней.	Нет
Windows 98	Преобразование не выполняется. Файловая система остается прежней.	Нет

Альтернативная загрузка Windows 2000

Возможность доступа к томам NTFS при альтернативной загрузке Windows 2000 с Windows NT зависит от версии последней. Тома NTFS, доступные через сеть на файловых серверах и серверах печати, не преобразуются при обновлении ОС компьютера клиента до Windows 2000.

При альтернативной загрузке Windows 2000 с Windows NT 4.0 SP4 из последней может быть прочитан любой базовый том, отформатированный под NTFS в Windows 2000.

При альтернативной загрузке Windows 2000 с более ранними версиями Windows NT пользователь не сможет получить доступ к тому NTFS. Такие конфигурации включают:

- тома на съемных носителях;
- тома, используемые при альтернативной загрузке;
- общие тома в кластерных конфигурациях.

Совместимость NTFS

Из Windows NT 4.0 SP4 можно прочитать любой базовый (нединамический) том, отформатированный под NTFS в Windows 2000.

Драйвер NTFS для Windows NT 4.0 SP4 позволяет пользователям этой ОС монтировать тома NTFS 5.О. Впрочем, пользователи Windows NT 4.0 не могут задействовать расширенные возможности NTFS 5.О.

Если на компьютере, кроме Windows NT, установлена другая ОС, доступ к тому NTFS можно получить только из Windows NT. При этом остальные ОС должны использовать для системного и загрузочного раздела систему, отличную от NTFS.

Драйвер файловой системы Ntfs.sys

Новый драйвер файловой системы Ntfs.sys для Windows NT 4.0 поддерживает монтирование томов и альтернативную загрузку в смешанных с Windows NT средах. Из-за проблем совместимости альтернативная загрузка Windows NT 4.0 и Windows 2000 не рекомендуется. Драйвер NTFS для Windows NT 4.0 SP4 предназначен только для помощи в обновлении до Windows 2000.

Монтирование томов

Windows NT 4.0 не поддерживает монтирование томов NTFS 5.0. Windows 2000 автоматически модернизирует тома NTFS 4.0 до версии 5.0. При монтировании тома NTFS 5.0 под Windows NT 4.0 SP4 возможности NTFS 5.0 недоступны.

Системы с альтернативной загрузкой

Новый драйвер файловой системы NTFS предоставляет возможности альтернативной загрузки Windows NT 4.0 и Windows 2000. Для этого надо установить Windows NT 4.0 SP4. Впрочем, поскольку в Windows 2000 применяются другие дисковые структуры NTFS, такие утилиты Windows NT 4.0, как CHKDSK и AUTOCHK, в Windows 2000 не работают. Перед выполнением они проверяют версию файловой системы, поэтому после установки Windows 2000 надо использовать новые версии этих дисковых утилит.

Хотя при монтировании тома NTFS 5.0 под Windows NT 4.0 SP4 возможности NTFS 5.0 недоступны, операции чтения и записи, которые не используют функции NTFS 5.0, будут работать нормально.

Так как существует возможность чтения и записи файлов на том NTFS 5,0, Windows 2000 очищает том после его монтирования в Windows NT 4.0. Очистка обеспечивает согласованность структур данных NTFS 5.0 после монтирования тома в Windows NT 4.0.

Квотирование дисков

При работе в Windows NT 4.0 дисковые квоты Windows 2000 игнорируются, т. е. пользователь сможет занять больше дискового пространства, чем ему разрешено квотами в Windows 2000.

Если квота в Windows NT 4.0 превышена, Windows 2000 запретит нарушителям обращаться к диску. Пользователи по-прежнему смогут читать и записывать данные в существующие файлы, но не смогут увеличить их размеры — лишь удалить файлы и уменьшить их размер. Эти ограничения действуют, пока используемое пространство не сократиться до порога квоты.

Примечание Это обычное поведение системы контроля квот при активизации механизма квотирования. То же происходит при обновлении Windows NT 4.0 до Windows 2000 с включенными квотами.

Шифрование

В Windows NT 4.0 над зашифрованным файлом невозможно выполнять какие-либо операции, включая открытие, чтение, запись, копирование и удаление. Поскольку в Windows NT 4.0 доступ к зашифрованному файлу получить нельзя, дополнительно защищать его в Windows 2000 не требуется.

Разреженные файлы

В Windows NT 4.0 над разреженным файлом невозможно выполнять операции открытия, чтения, записи, копирования и удаления.

Идентификаторы объектов

В Windows NT 4,0 доступ к объектам Windows 2000 не ограничен. Над объектами можно выполнять операции чтения, записи, копирования и удаления. При удалении файла с идентификатором объекта Windows 2000 находит в индексе и удаляет соответствующую запись.

Журнал USN

В Windows NT 4,0 игнорируется, и доступ к файлам не регистрируется. По той же причине регистрируются не все изменения файлов. При загрузке Windows 2000 параметры журнала USN сбрасываются, указывая, что история журнала неполна. Приложения, использующие журнал USN, должны корректно взаимодействовать с незаполненными журналами. Все следующие попытки доступа в Windows 2000 будут регистрироваться, так что после монтирования тома под Windows 2000 журналу можно доверять.

Точки переопределения

В Windows NT 4.0 над зашифрованным файлом выполнять какие-либо операции, включая открытие, чтение, запись, копирование и удаление, невозможно.

Резюме

NTFS 5.0 поддерживает все возможности Windows 2000, включая точки переопределения, NSS и квотирование дисков. NTFS также поддерживает устройства хранения CDFS, UDF и DVD. В качестве фундаментальной единицы размещения информации NTFS использует кластер, состоящий из одного или нескольких секторов. Стандартный объем кластера зависит от размера раздела. Любой том NTFS содержит загрузочный сектор. Он начинается с нулевого сектора и занимает до 16 секторов. При форматировании тома под NTFS создаются таблица MFT (Master File Table) и метаданные. Каждый занятый сектор тома NTFS принадлежит файлу. Даже метаданные файловой системы являются частью файла. NTFS рассматривает каждый файл или каталог как набор атрибутов. Используя NTFS, примите во внимание такие факты, как обновление до Windows 2000, альтернативную загрузку Windows 2000 и вопросы совместимости NTFS.

Занятие 4. Безопасность файловых систем

Общие папки позволяют другим пользователям получить доступ к файлам Вашего компьютера. Они обеспечивают безопасность ресурсов и применяются на разделах FAT16, FAT32 и NTFS. NTFS поддерживает не только общие папки — разрешения NTFS позволяют определить полномочия каждого пользователя или группы в отношении конкретных ресурсов. Разрешения NTFS не доступны на разделах FAT.

Изучив материал этого занятия, Вы сможете:

- ✓ открывать общий доступ к папкам и назначать для них разрешения;
- ✓ назначать разрешения NTFS для файлов и папок.

Продолжительность занятия — около 35 минут.

Совместное использование папок

Общие папки (shared folders) предоставляют доступ к ресурсам других компьютеров в сети. Имея разрешение, пользователь может подключиться к общей папке и получить доступ к ее содержимому.

Разрешения доступа к общим папкам

Общие папки могут содержать приложения, данные или личные файлы пользователей. Каждый вид данных требует своего набора разрешений. В общем случае разрешения доступа к общим папкам обладают такими характеристиками;

- разрешения распространяются только на папки, но не на конкретные файлы, поэтому разрешения доступа к общим папкам — менее строгая мера защиты, чем разрешения NTFS;
- разрешения не распространяются на локальных пользователей — только на тех, кто обращается к общей папке по сети;
- назначение разрешений для общих папок — единственный способ защитить сетевые ресурсы в файловой системе FAT; разрешения NTFS недоступны на разделах FAT;
- по умолчанию группа Everyone (Все) получает для общей папки разрешения Full Control (Полный доступ).

В Windows Explorer (Проводник) под общей папкой изображена рука (рис. 4-9).

Рис. 4-9. Общие папки в Windows Explorer (Проводник)

Для каждой общей папки можно назначить свои разрешения. Разрешения контролируют действия пользователей над общими ресурсами. В таблице перечислены действия пользователей, предусмотренные каждым разрешением. Разрешения расположены в порядке убывания строгости ограничений.

Каждому пользователю или группе можно предоставить доступ к общей папке. Вообще лучше предоставлять разрешения группе, чем отдельному пользователю. Явно аннулировать разрешения следует, только когда надо переопределить наследуемые разрешения. Например, можно аннулировать разрешения члена группы, обладающей данным разрешением. При аннулировании разрешений пользователь теряет доступ к ресурсу.

Разрешение	Описание
Read (Чтение)	Пользователи могут просматривать содержимое файлов и папок, атрибуты файлов, запускать программы и менять папки внутри общей папки.
Change (Изменить)	Пользователи могут создавать папки и файлы, добавлять и изменять данные в файлах, изменять атрибуты файлов, удалять файлы и папки, а также выполнять действия, предусмотренные разрешением Read.
Full Control (Полный доступ)	Пользователи могут изменять права доступа к файлам и владельцев **файлов, а также выполнять** действия, **предусмотренные разрешением Change.**

Назначение разрешений для общих папок

Разрешения для групп и пользователей регулируют доступ к общим папкам. Назначенные разрешения можно аннулировать.

Несколько разрешений

Пользователь может быть членом нескольких групп с разными разрешениями и разным уровнем доступа к общей папке. При этом его разрешения складываются из собственных разрешений и разрешений групп, в которые он входит. Например, если ему предоставлены разрешения Read (Чтение), а его группе — Change (Изменить), фактически он будет обладать разрешением Change, которое включает и Read.

Аннулирование разрешений

Аннулирование разрешений блокирует ранее назначенные или наследуемые разрешения. Пользователь с аннулированными разрешениями не получит доступ к ресурсам, даже если он член полномочной группы.

Разрешения NTFS

В FAT для совместного использования ресурсов достаточно общих папок, но в **NTFS** общие папки — не лучшее решение. В FAT пользователь имеет доступ ко всему содержимому общей папки. В NTFS применяются либо разрешения доступа к общим папкам, либо разрешения **NTFS,** но не оба типа вместе. Разрешения NTFS предпочтительнее, поскольку их можно назначить не только для папок, но и для файлов. Если для папки назначены оба типа разрешений, учитываются более строгие.

Копирование или перемещение общей папки

При копировании общая папка остается общей, а ее копия — нет. Перемещенная папка перестает быть общей.

Рекомендации по использованию общих папок

- Определите группы, которым нужен доступ к каждому ресурсу, для каждой группы определите уровень доступа. Составьте список групп с разрешениями для каждого ресурса.
- Для упрощения администрирования предоставляйте разрешения группам, а не пользователям.
- Ограничивайте разрешения, насколько возможно. Например, если пользователи будут читать информацию, но никогда не будут удалять или создавать файлы, назначайте разрешения Read.

- Организуйте ресурсы так, чтобы ресурсы с одинаковым уровнем доступа находились в одной папке. Например, если пользователям нужны разрешения Read для нескольких папок с приложениями, храните их в одной папке — ей и назначайте разрешения.
- Чтобы пользователи могли свободно найти нужные им данные, применяйте понятные имена общих ресурсов. Имена должны поддерживаться ОС каждого клиента.

Примечание Клиенты MS-DOS, Windows 3.x и WFW поддерживают формат 8.3, поэтому в смешанных средах не применяйте длинные имена общих ресурсов.

Windows 2000 поддерживает эквивалентные имена файлов в формате 8.3, которые могут быть непонятны пользователям. Например, папка Accountants Database на компьютерах клиентов, использующих MS-DOS, Windows 3.x или Windows for Workgroups, будет иметь имя Accoun~1.

Общий доступ к папкам

Чтобы сделать ресурсы Вашего компьютера доступными для других пользователей, надо создать общие папки. Для этого Вы должны быть членом одной из привилегированных групп в зависимости от роли компьютера, где расположены ресурсы. Ограничив число пользователей, которые могут одновременно подключаться к общей папке, и предоставив разрешения отдельным пользователям и группам, Вы сможете контролировать их доступ к общей папке и ее содержимому. Тогда, чтобы получить доступ к общей папке, пользователи должны иметь соответствующие права. Свойства общих папок можно изменять, например можно прекратить совместное использование папки, изменить сетевое имя или разрешения.

Требования для открытия доступа к папке

В Windows 2000 открывать доступ к папке вправе только члены встроенных групп Administrators (Администраторы), Server Operators (Операторы сервера) и Power Users (Опытные пользователи). Какие группы могут выделять общие папки на конкретном компьютере, зависит от его роли в сети и принадлежности к рабочей группе или домену.

- В домене Windows 2000 группы Administrators и Server Operators могут выделять общие папки на любом компьютере домена. Группа Power Users является локальной, поэтому ее члены могут выделять общие папки только на изолированном сервере или компьютере с Windows 2000 Professional, где расположена группа.
- В рабочей группе Windows 2000 группы Administrators и Power Users могут открывать доступ к папке на изолированном сервере Windows 2000 Server или компьютере с Windows 2000 Professional, где расположена группа.
- Пользователи с привилегией Create Permanent Shared Objects (Создание постоянных объектов совместного использования) могут открывать доступ к папкам на компьютерах, где им предоставлено это право.

Примечание Если папка, которую надо сделать общей, находится на томе NTFS, пользователи должны обладать хотя бы разрешением Read.

Административные общие папки

Для упрощения администрирования Windows 2000 автоматически создает несколько общих папок. К имени стандартных общих папок добавляется знак доллара ($), скрываю-

ший общие папки от пользователей, подключающихся к компьютеру. Скрытыми общими папками являются корни каждого тома, системная папка и папка с драйверами принтеров.

Административные общие папки, автоматически генерируемые Windows 2000, перечислены ниже.

Общая папка	Описание
CS, D$, E$...	Корень каждого тома на жестком диске. Сетевым именем является буква диска со знаком доллара ($) на конце. Подключаясь к такой папке. Вы получаете доступ ко всему тому. Эти папки предназначены для выполнения административных задач, для чего группе Administrators предоставляются разрешения Full Control (Полный доступ). Съемные устройства, например CD-ROM, скрытыми общими папками не являются.
Admin$	Системная папка, по умолчанию C:\Winnt, предназначена для управления Windows 2000 с удаленного компьютера, при этом администратор может не знать, в какую папку установлена ОС. Доступ к этой папке могут получить только члены группы Administrators с разрешением Full Control.
Print$	При установке первого сетевого принтера папка %systemroot%\System32\ Spool\Drivers, где находятся драйверы принтеров, становится общей. Группы Administrators, Server Operators и Print Operators (Операторы печати) обладают разрешениями Full Control. Группа Everyone (Все) обладает разрешением Read.

Скрытые общие папки не ограничиваются теми, что система создает автоматически. Вы можете сами создать скрытую общую папку, добавив знак $ к ее сетевому имени. И доступ к папке получат полномочные пользователи, знающие ее сетевое имя.

Открытие доступа к папке

При этом можно указать ее сетевое имя, комментарии по содержимому, ограничить число одновременно обращающихся пользователей и назначить разрешения. Вы также вправе открыть доступ к папке под несколькими сетевыми именами. Чтобы сделать папку общей, щелкните ее правой кнопкой и выберите в контекстном меню команду Properties (Свойства). В открывшемся диалоговом окне свойств папки надо перейти на вкладку Sharing (Доступ) (рис. 4-10).

В таблице перечислены параметры вкладки Sharing;

Параметр	Описание
Do Not Share This Folder I Отменить общий доступ к этой папке)	Если выбран этот переключатель, папка общей не будет. Остальные параметры вкладки станут недоступными.
Share This Folder (Открыть общий доступ к **этой папке)**	Если отмечен этот переключатель, папка будет считаться общей, а остальные параметры станут доступными.
Share Name (Сетевое имя)	Сетевое имя, которое будут указывать пользователи для обращения к папке через сеть. Обязательный параметр.
User Limit (Предельное число пользователей)	Максимальное число пользователей, которые могут одновременно подключаться к общей папке. Если выбран параметр Maximum Mowed (Максимально возможное), Windows 2000 Server будет поддерживать неограниченное число соединений. Впрочем, это количество ограничено приобретенными клиентскими лицензиями доступа.

(окончание)

Параметр	Описание
Comment (Комментарий)	Описание сетевого ресурса. Отображается при просмотре общих папок с клиентских компьютеров, обычно используется для описания их содержимого.
Permissions (Разрешения)	Разрешения для общей папки. Действуют только при доступе через сеть. По умолчанию группа Everyone получает для новой папки право Full Control.
Caching (Кэширование)	Определяет способ локального кэширования файлов общей папки при доступе с удаленного компьютера.
New Share (Новый общий ресурс)	Позволяет создать новую общую папку.
Remove Share (Удалить общий ресурс)	Позволяет удалить общую папку. Доступен только для общих пэпок.

Выделив общую папку, надо указать пользователей, которые получат к ней доступ. Это можно сделать, предоставив разрешения отдельным пользователям и группам. Для этого в диалоговом окне свойств папки щелкните кнопку Permissions (Разрешения) на вкладке Sharing (Доступ). В открывшемся окне выберите пользователей или группы, которым надо предоставить разрешения.

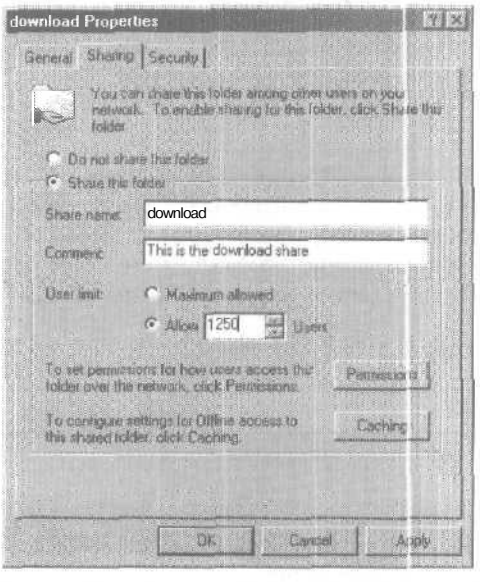


Рис. 4-10. Вкладка Sharing (Доступ) диалогового окна свойств папки

Изменение свойств общей папки

Свойства общих папок можно изменять, например, можно прекратить совместное использование папки, изменить сетевое имя или разрешения. Для этого служит диалоговое окно свойств папки. Чтобы изменить соответствующие свойства папки:

Изменение	Действия
Прекращение совместного использования папки	Выберите переключатель Do Not Share This Folder (Отменить обший доступ к этой папке).
Изменение сетевого имени	Сначала щелкните переключатель Do Not Share This Folder, чтобы прекратить совместное использование папки. Чтобы изменения вступили в силу, щелкните кнопку Apply (Применить), затем — переключатель Share This Folder (Открыть общий доступ к этой папке). В поле Share Name (Сетевое имя) введите новое сетевое имя.
Изменение разрешений	Щелкните кнопку Permissions (Разрешения). В диалоговом окне настройки разрешений щелкните кнопку Add (Добавить) или Remove (Удалить). Щелчок кнопки Add откроет диалоговое окно Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы), где можно выбрать нового пользователя или группу.
Создание дополнительного сетевого имени	Щелкните кнопку New Share (Новый общий ресурс). Дополнительное сетевое имя понадобится, если Вы хотите объединить несколько общих папок и при этом дать возможность пользователям применять старое сетевое имя.
Удаление сетевого имени	Щелкните кнопку Remove Share (Удалить общий ресурс). Эта кнопка отображается, если у папки минимум два сетевых имени.

Примечание Если в момент отмены общего доступа к папке есть открытые файлы, пользователи потеряют данные. В этом случае после щелчка кнопки Apply появится предупреждение, что к папке подключены пользователи.

Разрешения NTFS

Это стандартный набор прав, предоставляющих или запрещающих доступ к ресурсам. В NTFS можно назначать разрешения не только для папок, но и для отдельных файлов, а также указать вид самого доступа. Кроме того, разрешения NTFS эффективны при доступе как с удаленного, так и с локального компьютера.

Стандартные разрешения NTFS в Windows NT:

- **разрешения доступа к папкам** обеспечивают безопасность папок на томе NTFS;
- **разрешения доступа к файлам** обеспечивают безопасность файлов на томе NTFS.

Назначение разрешений NTFS

Разрешение Full Control

Предоставляет полный доступ к ресурсу. По умолчанию назначается так:

- пользователь, создавший файл или папку, получает статус Creator Owner (Создатель-владелец) и разрешение Full Control (Полный доступ);
- при форматировании тома под NTFS, группе Everyone предоставляется разрешение Full Control для корня этого тома;
- при преобразовании разделов FAT в NTFS, группе Everyone предоставляется разрешение Full Control для всех ресурсов этого раздела,

Несколько разрешений NTFS

Разрешения предоставляются группам и пользователям, поэтому нередко член одной или нескольких групп имеет разные разрешения. В этом случае права пользователя складываются из собственных разрешений и разрешений группы, к которой он принадлежит. Например, если ему дано право Write (Запись), а его группе — Read (Чтение), он обладает обоими.

Разрешения доступа к файлам в NTFS имеют приоритет над разрешениями доступа к папкам. Так, пользователь, имеющий разрешение Write для папки и Change (Изменить) для файла внутри этой папки, обладает обоими разрешениями для данного файла. Это правило справедливо также, когда пользователю запрещен доступ к папке. Имея разрешение, пользователь всегда получит доступ к файлам из приложения на основе их полного UNC-имени или пути. Например, если пользователю запрещен доступ к папке, но предоставлено разрешение Change для файла внутри нее, он сможет открыть файл из приложения, указав его полное UNC-имя или путь к файлу.

Аннулирование разрешений блокирует разрешения пользователя, даже если они предоставлены группе, к которой он принадлежит. Так, если группе Everyone дано разрешение Full Control для файла, а ее члену запрещено удалять этот файл, то он сможет читать и изменять, но не удалить файл.

Наследование разрешений

По умолчанию разрешения для родительской папки наследуются для всех ее подпапок и файлов. При назначении или изменении разрешений для папки разрешения применяются к самой папке и всех вложенных и впоследствии создаваемых в ней папок и файлов. Унаследованные разрешения можно изменить или удалить. Впрочем, наследование разрешений от родительской папки можно отключить, после чего явно задать их для вложенных папок и файлов. Унаследованные разрешения можно также изменить или удалить.

Рекомендации по назначению разрешений NTFS

- Для упрощения администрирования сгруппируйте ресурсы в папки приложений, данных и личных данных пользователей. Это даст три преимущества:
  - разрешения можно назначить не отдельным файлам, а целым папкам;
  - упрощается процесс архивирования;
  - личные данные всех пользователей расположены в одном месте.
- Разрешения должны быть максимально строгими. Это снизит вероятность случайного удаления или изменения важной информации.
- Назначайте разрешения группам, а не отдельным пользователям, когда это возможно. Создавайте группы, исходя из требуемого уровня доступа, и предоставляйте им соответствующие права. Предоставляйте разрешения отдельным пользователям, только когда это действительно надо.
- Личные папки пользователей лучше поместить отдельно от приложений и системных файлов. Это упростит архивирование и администрирование.
- При назначении разрешений для папок, где содержатся рабочие данные или приложения, аннулируйте разрешение Full Control для группы Everyone и предоставьте разрешения Read & Execute (Чтение и выполнение) группам Users (Пользователи) и Administrators (Администраторы). Это предотвратит случайное удаление файлов или их заражение вирусами. Администраторам и пользователям, ответственным за обновление ПО, можно разрешить Full Control, а по завершении обслуживания снова предоставить Read & Execute.
- Для папок с совместно используемыми данными предоставляйте разрешения Add (Дозапись) и Read & Execute группе Users и разрешение Full Control пользователям со ста-

тусом Creator Owner. В этом случае пользователи смогут читать любые документы, но удалить или изменить смогут только файлы и папки, которые они сами создали.

- Вообще лучше назначать, чем аннулировать разрешения, поэтому последнее лучше делать, только когда надо блокировать определенный вид доступа для конкретного пользователя или группы.
- Пользователи должны научиться назначать разрешения для файлов и папок, которые они создали и которыми владеют. Ознакомьте их с правилами назначения разрешений.

Настройка разрешений NTFS

Администраторы и владельцы файлов и палок могут предоставить пользователям и группам доступ к ресурсам.

Чтобы назначить или изменить разрешения файлов или папок, откройте диалоговое окно свойств нужного ресурса. Разрешения NTFS настраиваются на вкладке Security (Безопасность). Ее элементы:

Элемент	Описание
Name (Имя)	Список пользователей и групп с разрешениями для данного ресурса. Щелкните учетную запись пользователя или группу, чтобы назначить/изменить разрешения или удалить ее из списка.
Permissions (Разрешения)	Разрешения, которые можно назначить или аннулировать. Пометьте флажок Allow (Разрешить), чтобы назначить разрешение, или флажок Deny (Запретить), чтобы его аннулировать.
Add (Добавить)	Позволяет добавить пользователя или группу в список Name.
Remove (Удалить)	Удаляет выбранного пользователя или группу и связанные с ними разрешения.
Allow Inheritable Permissions From Parent To Propagate that To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект)	По умолчанию флажок не отмечен. Это значит, что подпапки не наследуют разрешений родительской папки. Для файлов этот параметр задан, так что вложенные файлы автоматически наследуют разрешения родительской папки.
Advanced (Дополнительно)	Открывает диалоговое окно Access Control Settings (Параметры управления доступом), где настраиваются специальные разрешения, аудит и принадлежность файлов и папок.

Специальные разрешения

Обычно стандартных разрешений NTFS хватает, чтобы обеспечить безопасность данных. Однако бывает, что их недостаточно. Тогда применяются специальные разрешения NTFS. Их, как и стандартные, можно предоставить либо аннулировать.

Специальные разрешения позволяют более тонко контролировать доступ к ресурсам. Существует 13 специальных разрешений, комбинациями которых являются стандартные разрешения Read & Execute, Modify (Изменить) и Full Control. Например, стандартное разрешение Read включает в себя разрешения Read data (Чтение данных), Read attributes (Чтение атрибутов) и Read extended attributes (Чтение дополнительных атрибутов).

Задание специальных разрешений для папок и файлов включает три задачи:

- более тонкую настройку разрешений;
- смену владения;
- аудит доступа.

Изменение разрешений

Назначать разрешения вправе владельцы ресурсов и другие пользователи с разрешением Full Control. Кроме того, можно сделать так, чтобы администраторы сети, не обладая Full Control, могли назначать разрешения. Для этого предоставьте группе администраторов сети специальные разрешения Change Permissions (Смена разрешений) — тогда они смогут назначать разрешения, но не смогут удалять файлы и папки или записывать в них данные.

Если член группы Administrators становится владельцем файла или папки, то владельцем считается вся группа, и любой ее член может получить доступ или изменить разрешения.

Смена владения

Кроме разрешений, можно сменить владельцев файлов и папок. Это достигается следующими способами.

- Текущий владелец ресурсаможет предоставить другим пользовагелям стандаргное разрешение Full Control или специальное — Take Ownership (Смена владельца), позволив им завладеть ресурсом.
- Администраторы могут стать владельцами любых файлов и папок, находящихся под их контролем. Например, если служащий покидает компанию, администратор может стать владельцем его файлов и изменить разрешения, чтобы другие пользователи получили доступ к ресурсам.
- Первоначально действие специальных разрешений, назначаемых для тома или папки, распространяется только на уровень, указанный в списке Apply Onto (Применять), который подробно обсуждается далее.

Чтобы сменить владельца папки или файла, откройте диалоговое окно Access Control Settings (Параметры управления доступом) и перейдите на вкладку Owner (Владелец). Текущий владелец ресурса указан в поле Current Owner Of This Item (Текущий владелец этого элемента). В списке Change Owner To (Изменить владельца на) выберите нового владельца. Можно изменить и владельца всех подпапок и файлов внутри данной папки, пометив флажок Replace Owner On Subdirectories And Objects (Заменить владельца субконтейнеров и объектов).

Назначение специальных разрешений

Чтобы назначить специальные разрешения, откройте диалоговое окно свойств файла или папки, перейдите на вкладку Security (Безопасность) и щелкните кнопку Advanced (Дополнительно). Откроется диалоговое окно Access Control Settings (Параметры управления доступом). Выберите вкладку Permissions (Разрешения) и щелкните кнопку Add (Добавить), чтобы добавить нового пользователя или группу и изменить специальные разрешения. Чтобы предоставить специальные разрешения пользователю или группе, щелкните кнопку View/Edit (Показать/изменить). Здесь Вы можете настроить специальные разрешения с помощью следующих параметров.

Параметр	Описание
Name (Имя)	Учетная запись пользователя или имя группы. Чтобы изменить пользователя или группу, щелкните кнопку Change (Изменить).

(окончание)

Параметр	Описание
Apply Onto (Применять)	Уровень иерархии, согласно которому наследуются специальные права доступа NTFS. По умолчанию — This Folder, Subfolders, and Files (Для этой папки, ее подпапок и файлов).
Permissions (Разрешения)	Специальные разрешения. Пометьте флажки Allow (Разрешить) или Deny (Запретить), чтобы предоставить или аннулировать специальные разрешения.
Apply These Permissions To Objects And/Or Containers Within This Container Only (Применять эти разрешения к объектам и контейнерам только внутри этого контейнера)	Флажок доступен при назначении специальных разрешений для папок и подпапок. Если пометить его, разрешения данной папки будут наследоваться нижестоящими папками. Действие этого флажка не распространяется на файлы.
Reset Permission On АЛ Child Objects And Enable Propagation Of Inheritable permissions (Переносить наследуемые от родительского объекта разрешения на этот объект)	Флажок доступен при назначении специальных разрешений для раздела. Пометив его, Вы переназначите разрешения для всех папок, подпапок и файлов этого раздела. Если флажок помечен, доступен флажок Apply These Permissions To Objects And/or Containers Within This Container Only.
Clear all (Очистить все)	Сбрасывает все выбранные разрешения и уровень наследования разрешений.

Ниже перечислены параметры раскрывающегося списка Apply Onto.

Параметр	Объекты, на которые распространяются права доступа
This Folder Only (Только для этой папки)	Только на папку.
This Folder, Subfolders, And Files (Для этой папки, ее подпапок и файлов)	На папку, подпапку и файлы. Файлы и папки, впоследствии создаваемые в данной папке, будут наследовать права доступа.
This Folder And Subfolders (Для этой папки и ее подпапок)	На папку и подпапки. Файлы и папки, впоследствии создаваемые в данной папке и ее подпапках, будут наследовать права доступа.
This Folder And Files (Для этой папки и ее файлов)	На папки и файлы. Файлы и папки, впоследствии создаваемые в данной папке, будут наследовать права доступа.
Subfolders And Files Only (Только для подпапок и файлов)	На подпапки и файлы. Файлы и папки, впоследствии создаваемые в подпапках данной папки, будут наследовать права доступа.
Subfolders Only (Только для подпапок)	На подпапки. Папки, впоследствии создаваемые в подпапках, будут наследовать права доступа.
Files Only (Только для файлов)	Только на файлы.

Копирование и перемещение файлов и папок

NTFS позволяет копировать и перемешать общие файлы и папки.

Копирование файлов и папок

Для копирования файлов и папок между томами NTFS или внутри тома пользователь должен иметь разрешение Add для папки назначения. Пользователь, выполняющий операцию копирования, становится владельцем новой папки или файла.

При копировании файла права доступа наследуются или теряются в зависимости от того, куда копируется папка;

- при перемещении файлов и папок в рамках одного раздела NTFS права доступа сохраняются;
- при копировании файлов и папок в рамках одного раздела NTFS, копировании или перемещении файлов и папок на другой раздел NTFS права доступа наследуются от папки назначения;
- при копировании файлов на тома FAT права доступа NTFS теряются.

Перемещение файлов и папок

Чтобы перемещать файлы/папки между разделами NTFS, требуется разрешение Add для папки/файла назначения и разрешение Delete (Удаление) для исходного файла/папки. Разрешение Delete необходимо, поскольку после копирования файл/папка удаляются из исходной папки. Пользователь, выполнивший перемещение, получает статус Creator Owner.

При перемещении файлов/папок между томами NTFS первоначальные разрешения могут измениться. Возможные результаты перемещения файла или папки:

Действие	Результат
Перемещение внутри тома	Папки и файлы сохраняют старые разрешения.
Перемещение на другой том	Папки и файлы унаследуют разрешения родительской папки.

При перемещении на разделы FAT файлы и папки теряют разрешения NTFS.

Примечание В главе 7 Вы научитесь регистрировать пользователей и группы и предоставлять им разрешения.

Устранение типичных проблем с разрешениями NTFS

Проблема	Возможная причина и устранение
Пользователь не может получить доступ к файлу или папке.	Проверьте разрешения пользователя и его группы. Если они аннулированы, пользователь не получит доступ к ресурсу. При копировании файла/папки разрешения могут измениться из-за наследования разрешений родительской папки. Если для палки заданы разрешения доступа к общим папкам и разрешения NTFS, будут применяться более строгие. Поэтому лучше предоставить группе Everyone разрешение Full Control и контролировать доступ только с помощью разрешений NTFS.

(*окончание*)

Проблема	Возможная причина и устранение
Пользователь не получает доступ к файлу или папке при добавлении его учетной записи в полномочную группу.	Каждый раз при регистрации пользователя в Windows NT или Windows 2000 генерируется маркер доступа. Чтобы пользователь мог подключиться к компьютеру, надо обновить информацию о группах, к которым он принадлежит. Для этого пользователь должен либо выйти, а затем снова войти в систему, либо закрыть все соединения, а затем снова открыть их.
Пользователь может удалить файл, не обладая на то полномочиями.	Назначайте разрешения на уровне папок, а не отдельных файлов. Чтобы запретить доступ пользователей, поместите файлы в отдельную папку и назначьте для нее наиболее строгие разрешения. Если проблема осталась, не предоставляйте для этой папки разрешение Full Control. Вместо этого, назначьте все остальные разрешения: Modify, Read & Execute, List Folder Contents (Список содержимого папки), Read и Write. Назначение этих разрешений эквивалентно назначению Full Control за исключением того, что пользователь не сможет удалять файлы.

Резюме

Общие палки позволяют другим пользователям получить доступ к файлам Вашего компьютера по сети. Впрочем, доступ к содержимому общей папки могут получить лишь полномочные пользователи. Разрешения доступа к общим папкам не распространяются на файлы и применяются только на уровне папок. При открытии доступа к папке указывается ее сетевое имя, комментарий, максимальное число одновременно обращающихся пользователей, разрешения и дополнительные сетевые имена. Разрешения доступа к общим папкам — это единственный способ защитить ресурсы на разделах FAT, для которых неприменимы разрешения NTFS. Они являются набором стандартных прав, которые предоставляют или запрещают доступ к ресурсам. По умолчанию разрешения, назначаемые для разделов и папок, не распространяются на внутренние подпапки и файлы. Разрешения доступа предоставляют администраторы и владельцы ресурсов.

Закрепление материала

? J Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Как установить новый жесткий диск объемом 10 Гб, который надо разбить на 5 секций по 2 Гб каждая?

2. Вы хотите создать чередующийся том на компьютере с Windows 2000 Server. У Вас хватает неразмеченного пространства на двух дисках, но в контекстном меню для свободного места доступна только команда создания нового раздела. В чем проблема и как ее решить?

3. Ваш компьютер способен загружать Windows 98 и Windows 2000. Вы преобразовали один из дисков с архивными файлами из базового в динамический. После этого из Windows 98 прочесть файл с этого диска стало невозможно. В чем причина?

4. Какие разрешения назначаются по умолчанию при форматировании раздела под NTFS? Кто сможет получить доступ к этому разделу?

5. Назовите эффективные разрешения пользователя, если ему предоставлено разрешение Write, а его группе — Read для одной и той же папки.

6. Что происходит с разрешениями файла при его перемещении из одной папки в другую в рамках одного раздела NTFS? Что происходит при перемещении файла на другой раздел NTFS?

7. Как сменить владельца файлов и папок увольняющегося сотрудника?

8. Назовите лучший способ обеспечить безопасность общих ресурсов на разделе NTFS.

ГЛАВА 5

Дополнительные файловые системы

В этой главе

Здесь рассматриваются *распределенная файловая система* (distributed file system, DFS) и *служба репликации файлов* (File Replication Service, FRS). DFS позволяет упростить доступ к файлам, физически расположенным в разных частях сети. DFS представляет файлы разных серверов так, как если бы они находились на одном компьютере. При этом пользователям не требуется знать и указывать их физическое расположение. Для синхронизации содержимого между назначенными репликами DFS применяется *служба репликации файлов* (FRS), Оснастка Microsoft Active Directory Sites and Services (Active Directory — сайты и службы) использует FRS для репликации сведений о топологии и информации глобального каталога между контроллерами домена.

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить упражнения всех предыдущих глав, чтобы оба компьютера работали под управлением Windows 2000 Server и были настроены в соответствии с приведенными инструкциями.

Занятие 1. Распределенная файловая система

DFS обеспечивает удобный доступ к. общим папкам, находящимся в разным частях сети. Общий каталог DFS является централизованным входом для доступа к остальным общим каталогам сети.

Изучив материал этого занятия, Вы сможете:

- ✓ сконфигурировать изолированный корень DFS;
- ✓ настроить DFS-ссылку;
- ✓ создать отказоустойчивый корень DFS.

Продолжительность занятия — около 35 минут.

Общие сведения о DFS

DFS представляет собой единую логическую иерархическую файловую систему. Она организует общие папки разных компьютеров сети в логическое дерево (рис. 5-1).

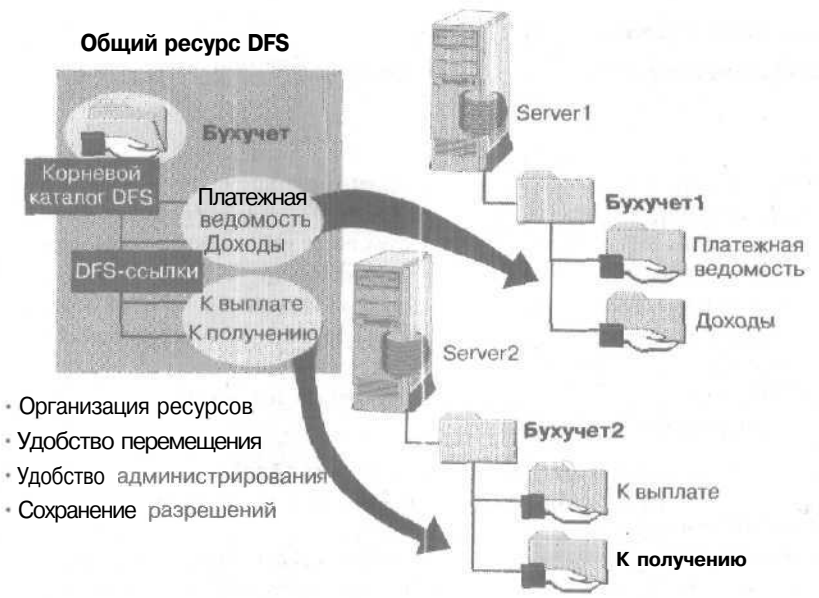


Рис. 5-1. Пример тома DFS

Поскольку дерево DFS является единой точкой доступа, пользователи могут обращаться к любым ресурсам сети независимо от расположения этих ресурсов. Как показано на рис. 5-1, ресурсы файловой системы, связанные с бухгалтерским учетом и находящиеся на различных серверах, организованы в единый логический корневой каталог DFS с именем Бухучет.

Пользователю, просматривающему общую папку под управлением DFS, не надо знать имя сервера, на котором она находится. Это упрощает доступ к сети, поскольку указывать расположение сервера, содержащего нужный ресурс, не требуется: достаточно подключится к корневому каталогу DFS. В нашем примере пользователи найдут все бухгалтерские документы в одном месте.

Древовидная структура томов DFS включает корень и ссылки. Для создания тома DFS надо сначала создать корень DFS. Любой корневой каталог DFS может содержать несколько DFS-ссылок, указывающих на общие папки, размещенные на разных серверах сети. DFS-ссылки корневого каталога DFS представляют общие папки (*<имя_компьютера>\<имя_общего_ресурса>*), которые физически могут находиться на разных файловых серверах.

Ниже перечислены преимущества DFS.

Функция	Описание
Администрирование сети	DFS упрощает администрирование. При отказе сервера Вы можете незаметно для пользователей изменить DFS-ссылку, чтобы она указывала на общую папку на другом сервере. Для пользователей путь к DFS-ссылке останется прежним.
Пространство имен	В отличие от обычной файловой системы, где назначаются логические имена дисков, клиенты обращаются к файловым ресурсам, используя единое пространство имен (корень DFS).
Экономия памяти	Клиентам Windows 2000 и Windows NT 4.0 не нужен дополнительный объем памяти, так как поддержка DFS встроена в клиентский перенаправитель этих ОС. Чтобы обеспечить 32-разрядному клиенту Windows доступ к общему каталогу DFS, в Windows 9x надо установить службу DFS Service for Microsoft Network Client.
Расширяемость	Пространство имен DFS можно расширить согласно новым требованиям организации или для предоставления дополнительного дискового пространства.
Замена сервера	DFS позволяет администраторам заменять файл-серверы, не затрагивая пространство имен, используемое сетевыми клиентами. Для этого надо лишь изменить путь к серверу из оснастки Distributed File System (Распределенная файловая система DFS).
Распределение нагрузки	DFS обеспечивает определенный уровень отказоустойчивости и позволяет распределять нагрузку, поскольку клиенты произвольно выбирают искомый физический сервер из списка альтернатив, возвращаемого сервером DFS.
Сетевые разрешения	DFS сохраняет сетевые разрешения. Каких-либо дополнительных разрешений или системы защиты не требуется, так как тома DFS используют существующие разрешения Windows 2000 для файлов и каталогов. Списки управления доступом (ACL) для отказоустойчивых реплик реплицируются.
Кэширование информации клиентами	Клиенты DFS кэшируют ссылки на часто используемые сетевые ресурсы, не тратя времени на поиск серверов. При первом обращении к дереву DFS производительность слегка падает (как при использовании команды Net Use). Кэширование позволяет избежать снижения производительности при следующих обращениях к этой области дерева до перезапуска клиентской системы или очистки кэша.
Интеграция с Internet Information Services	DFS взаимодействует с IIS. При условии, что администратор нужным образом перенастроит DFS, при физическом перемещении исходной Web-страницы с одного сервера на другой изменять имеющиеся на ней ссылки на другие Web-страницы, хранящиеся в разделах DFS, не требуется.

Ограничения, накладываемые DFS

Элемент	Ограничение
Максимально допустимое количество символов в пути	260
Максимально допустимое количество альтернативных ресурсов в томе	32
Максимально допустимое количество корневых каталогов DFS на сервере	1
Максимально допустимое количество корневых каталогов DFS в домене	Не ограничено
Максимально допустимое количество томов в домене или на предприятии	Ограничивается ресурсами системы. Имеется успешный опыт использования 6 000 томов в изолированных корнях.

Примечание В статье «Distributed File System: A Logical View Of Physical Storage» дан обзор альтернативных технологий и многих аспектов использования DFS. См. документ \chapt05\articles\DFS New.doc на прилагаемом компакт-диске.

Типы корней DFS

Служба DFS устанавливается автоматически вместе с Windows 2000 Server. Ее можно переводить в режим паузы, останавливать и повторно запускать; однако удалить службу DFS из ОС нельзя.

На компьютере Windows 2000 Server можно сконфигурировать два типа корней DFS: изолированные и доменные (или отказоустойчивые корни DFS).

Изолированные корни DFS

Ниже перечислены общие характеристики изолированных корневых каталогов DFS,

- Информация изолированной DFS хранится в локальном реестре.
- В изолированном корне DFS разрешается создать только один уровень DFS-ссылок.
- Если подключение к изолированным корням DFS производится из оснастки Distributed File System (Распределенная файловая система DFS), возвращаются имена всех серверов из списка просмотра, поскольку DFS-серверы не регистрируют уникальных имен NetBIOS.
- Изолированные корни DFS можно размешать на дисках с любыми поддерживаемыми файловыми системами, хотя рекомендуется выбирать для них разделы NTFS.
- Изолированные корни DFS не поддерживают репликацию и резервное копирование, а потому являются потенциальным источником сбоя; для изолированного корня DFS можно создать реплику. Однако репликация таких корней не поддерживается.

Доменные корни DFS

Ниже перечислены характеристики отказоустойчивых корней DFS.

- В доменных корнях ссылки на пространство имен DFS обрабатываются несколькими серверами. Для хранения древовидной топологии DFS и обеспечения отказоустойчивости корня применяется Active Directory.

- Отказоустойчивый корень хранится в Active Directory и тиражируется на все задействованные серверы-корни DFS. Active Directory обеспечивает автоматическую синхронизацию изменений в дереве DFS. Это гарантия возможности восстановления древовидной топологии DFS при отключении корня DFS. Кроме того, отказоустойчивость можно реализовать на уровне файлов и содержимого путем включения в том DFS ресурсов-заместителей. Любую ветвь дерева DFS может обслуживать набор реплицированных ресурсов. Если соединиться с одним из таких ресурсов не удается, клиент DFS попытается подключиться к его реплике.
- Отказоустойчивые корни должны размещаться на разделах NTFS версии 5.0.
- Для DFS используется существующая топология репликации Active Directory.

Конфигурирование томов DFS

Windows 2000 позволяет конфигурировать изолированные корни DFS, DFS-ссылки и доменные корни DFS.

Создание изолированного корня DFS

Изолированный корень DFS хранит топологию DFS на отдельном компьютере. Данный вид DFS не обеспечивает отказоустойчивости при сбое этого компьютера или переносе одной из общих папок DFS.

Изолированный корень DFS должен физически размещаться на сервере, где регистрируются пользователи. Для создания изолированного тома DFS надо сначала создать корень DFS.

Чтобы создать изолированный корень DFS, из оснастки Distributed File System запустите мастер New DFS Root (Мастер создания нового корня DFS). На рис. 5-2 показано окно Select The DFS Root Type (Выбор типа корня DFS) с выбранным переключателем Create A Stand-Alone DFS Root (Создать изолированный корень DFS).

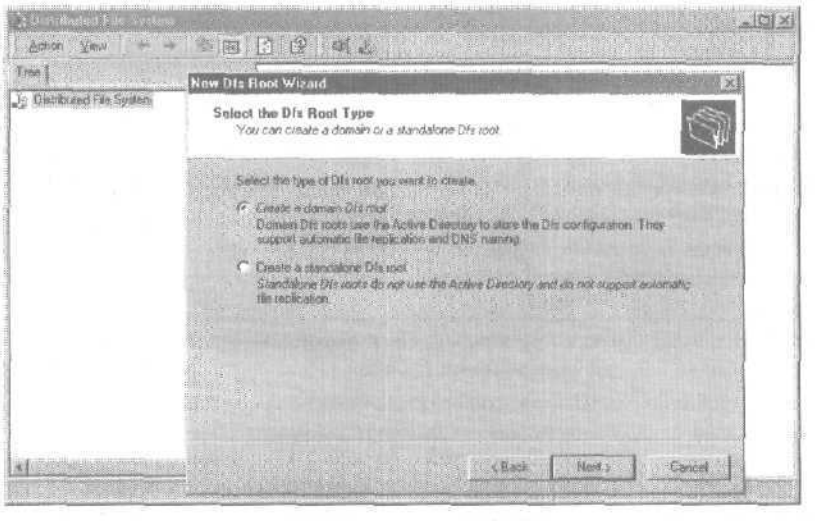


Рис. 5-2. Создание изолированного корня DFS из оснастки Distributed File System (Распределенная файловая система DFS)

Ниже описаны окна мастера и действия по созданию нового корня DFS.

Окно	Ваши действия
Select The DFS Root Type (Выбор типа корня DFS)	Щелкните переключатель Create A StandAlone DFS Root (Создать изолированный корень DFS), как показано на рис. 5-2.
Specify The Host Server For The DFS Root (Выбор несущего сервера для корня DFS)	Укажите начальную точку подключения для всех ресурсов дерева DFS. Корень DFS можно создать на любом компьютере Windows 2000.
Specify The DFS Share (Выбор общего ресурса для корня DFS)	Введите имя общей папки, где будет размещен корень DFS. Вы можете использовать имеющуюся папку или создать новую.
Name The DFS Root (Выбор имени для корня DFS)	В поле Comment text (Комментарий) введите описательное имя корня DFS.
Completing The New Root wizard (Завершение работы мастера создания нового корня DFS)	Просмотрите параметры настройки сервера (Host Server — Узловой сервер), а также поля Root Share (Корень) и Root Name (Имя корня). Чтобы внести изменения, щелкните кнопку Back (Назад). Завершив настройку, щелкните кнопку Finish (Готово).

Создание доменного корня DFS

Доменная DFS помешает топологию DFS в хранилище Active Directory. DFS-ссылки могут указывать на несколько идентичных обших папок (также называемых репликами), что обеспечивает отказоустойчивость. Кроме того, доменная DFS поддерживает DNS, множественные уровни дочерних томов я тиражирование файлов.

Для создания отказоустойчивого корня DFS также применяется мастер New DFS Root (Мастер создания нового корня DFS).

Создание DFS-ссылок

При просмотре папок корня DFS пользователям не требуется знать их физическое расположение. Создав корень, можно сконфигурировать DFS-ссылки (также называемые дочерними узлами).

Чтобы создать DFS-ссылку, откройте оснастку Distributed File System (Распределенная файловая система DFS) и шелкните нужный корень DFS. В меню Action (Действие) выберите команду New DFS Link (Создать ссылку DFS). Откроется диалоговое окно Create A New DFS Link (Создание новой ссылки DFS) (рис. 5-3).

Ниже описаны элементы диалогового окна Create A New DFS Link.

Элемент	Описание
Link Name (Имя ссылки)	Имя ветви корня DFS, которое пользователи увидят при подключении к DFS,
Send the user to this shared folder (Переадресовать пользователя на эту общую папку)	UNC-путь, сообщающий фактическое расположение общей папки, на которую указывает DFS-ссылка. Заметьте: у несущего сервера DFS должен иметься доступ ко всем общим папкам, упомянутым в DFS-ссылке.
Comment (Комментарий)	Необязательное описание папки (например ее действительное имя).
Clients cache this DFS referral for *x* seconds (Клиенты кэшируют ссылку каждые *x* секунд)	Период, в течение которого клиенты кэшируют разрешение DFS-ссылки. По истечении этого времени клиент повторно запрашивает сервер DFS о расположении DFS-ссылки, даже если ранее клиент уже устанавливал с ней соединение.

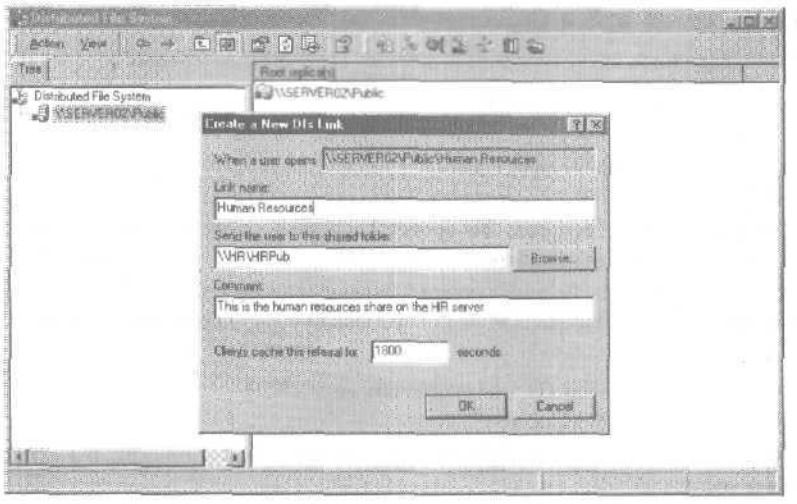


Рис. 5-3. Создание новой DFS-ссылки для папки отдела кадров

В оснастке Distributed File System ссылка появится в корневом томе **DFS;** для клиента DFS эта ссылка будет выглядеть, как папка корня DFS. На рис. 5-4 показан корень DFS с именем \\Server02\Public и DFS-ссылка на другой сервер.

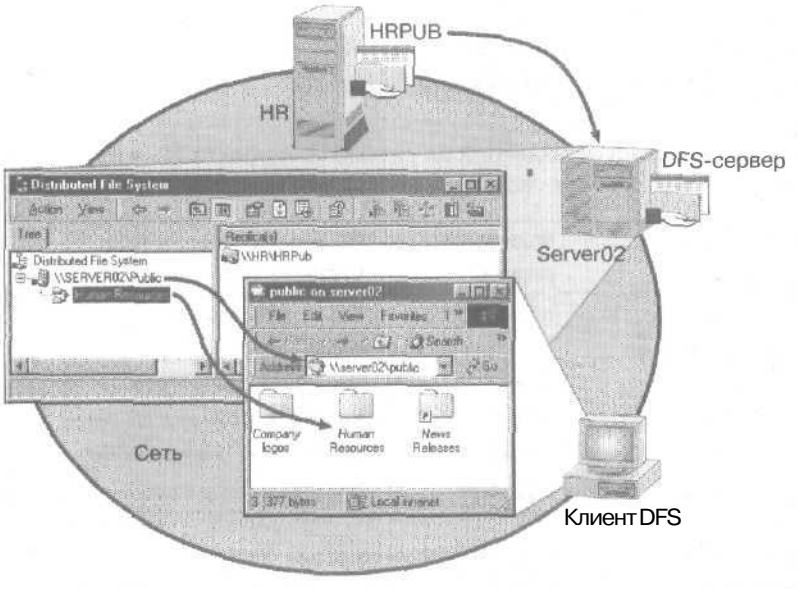


Рис. 5-4. **Вид корня DFS и DFS-ссылки в окне оснастки Distributed File System (Распределенная файловая система DFS), а также при просмотре клиентом DFS**

Упражнение: создание корня DFS и DFS-ссылки

Создайте общие каталоги, изолированный корень DFS и DFS-ссылки.

▶ Задание 1: создайте каталоги и общие ресурсы

Создайте новые папки или воспользуйтесь существующими каталогами, а затем сделаете их общими. Создать папки и общие ресурсы Вы можете любым удобным для Вас способом или выполнить описанные ниже действия.

1. Зарегистрируйтесь на Server01 как Administrator (Администратор) с паролем password.
2. Дважды щелкните значок My Computer (Мой компьютер) на рабочем столе.
   Откроется одноименное окно.
3. Дважды щелкните значок Local Disk (H:) [Локальный диск (H:)].
4. В меню File (Файл) выберите New (Создать), а затем — команду Folder (Папка).
   В окне Local Disk (H:) появится лапка с именем New Folder (Новая папка). В поле с именем папки будет мигать курсор.
5. Измените имя папки на Public.
6. Выделите папку Public и в меню File (Файл) выберите команду Sharing (Доступ).
   Откроется диалоговое окно Public Properties (Свойства: Public).
7. Щелкните переключатель Share This Folder (Открыть общий доступ к этой папке) и в поле Comment (Комментарий) введите **DFS root share.**
8. Щелкните OK.
   На значке папки Public появится изображение руки.
9. Повторите пп. 1–7, чтобы создать перечисленные ниже папки и общие ресурсы. Используйте разрешения по умолчанию.
   Помните, что иногда папки будут создаваться на дисках, отличных от H:, а в одном из случаев будет открыт общий доступ к папке на компьютере Server02.

Имя компьютера	Диск	Папка	Имя общего ресурса	Назначение/текст в поле Comment (Комментарий)
Server02	C:	\fnetpub\ wwwroot	Internal	Web-содержание для внутреннего пользования
Server01	I:	\Press	Press	Текущие пресс-релизы
ServerOl	C:	\Inetpub\ftproot	Ftproot	Корневой каталог FTP-узла
ServerOl	I:	\dev\TechDocs	Tech Docs	Техническая документация
ServerOl	C:	\Public\Press	Press Repl	Реплика текущих пресс-релизов

▶ Задание 2: создайте изолированный корень DFS на компьютере ServerOl

Создайте изолированный корень DFS, где будут размещены только что созданные общие ресурсы.

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и выберите пункт Distributed File System (Распределенная файловая система **DFS).**
   Откроется окно оснастки Distributed File System (Распределенная файловая система **DFS).**
2. Прочитайте сообщение на правой панели.

3. В меню Action (Действие) выберите команду New DFS Root (Создать корень DPS).
   Откроется окно мастера New DFS Root Wizard (Мастер создания нового корня DFS).
4. Прочтите информацию в первом окне мастера и щелкните Next.
5. В окне Select The DFS Root Type (Выбор типа корня DFS) Вам предлагается создать один из двух типов корней:
   - доменный, размещающий древовидную топологию DFS в хранилище Active Directory, поддерживающий DNS и тиражирование файлов;
   - изолированный, не использующий Active Directory и не поддерживающий автоматическое тиражирование файлов.

   Поскольку на данном этапе обучения Вы еще не настраивали контроллер домена, Вы создадите изолированный корень DFS.
6. Щелкните переключатель Create A Stand-Alone DFS Root (Создать изолированный корень DFS), а затем — Next.
7. Убедитесь, что в окне Specify The Host Server For The DFS Root (Выбор несущего сервера для корня DFS) выбран компьютер SERVER01, и щелкните Next.
   В окне Specify The DFS Root Share (Выбор общего ресурса для корня DFS) укажите разделяемый каталог, созданный в предыдущем упражнении.

   Заметьте: корень DFS можно разместить в существующей папке. Кроме того, при необходимости мастер может создать новый разделяемый каталог.
8. Убедитесь, что выбран переключатель Use An Existing Share (Использовать существующий общий ресурс), и из раскрывающегося списка выберите Public.
9. Щелкните Next.
10. В поле Comment (Комментарий) окна Name The DFS Root (Выбор имени для корня DFS) введите **Public** access **share** и щелкните Next.
11. В окне Completing The New DFS Root Wizard (Завершение работы мастера создания нового корня DFS) просмотрите параметры настройки и щелкните кнопку Finish (Готово),
    Откроется окно оснастки Distributed File System (Распределенная файловая система DFS), и на компьютере SERVER01 в папке Public будет создан корень DFS.

▶ **Задание 3: создайте DFS-ссылки**

Создайте DFS-ссылки в корне DFS с именем \\SERVER01\Public.

1. На левой панели оснастки Distributed File System выберите корень \\SERVER01\Public.
2. Раскройте меню Action (Действие) и убедитесь, что команды New Root Replica (Создать корневую реплику) и Replication Policy (Политика репликации) недоступны.
3. Выберите команду New DFS Link (Создать ссылку DFS).
   Откроется диалоговое окно Create A New DFS Link (Создание новой ссылки DFS).
4. В поле Link Name (Имя ссылки) введите intranet.
5. Щелкните кнопку Browse (Обзор).
   Откроется окно Browse For Folder (Обзор папок).
6. Щелкните значок «+» слева от Computers Near Me (Соседние компьютеры).
7. Щелкнув значок «+» слева от Server02, выберите internal и щелкните OK.
   В поле Send The User To This Shared Folder (Переадресовать пользователя на эту общую папку) будет указано \\Server02\internal.
8. В поле Comment (Комментарий) введите **Internal Web content** и щелкните OK.

9. Выполнение этого шага всегда начинайте с выбора корня \\SERVER01\Public в оснастке Distributed File System, Затем, повторяя пп. 3–8, создайте DFS-ссылки на основе представленной ниже информации.

Поле Link Name (Имя ссылки)	Поле Send The User To This Shared Folder (Переадресовать пользователя на эту общую папку)	Поле Comment (Комментарий)
News	\\Server01\Press	Current Press
ftp	\\Server01\ftproot	Ftp Root
Tech	\\Server01\TechDocs	Technical Documents Area

Примечание Вместо поиска общего ресурса Вы можете указать имя сервера и ресурса, используя стандартный синтаксис UNC.

► **Задание 4:** создайте **реплику DFS**

Создайте реплику DFS-ссылки News, указывающей на папку H:\Press (общий ресурс Press). Реплика будет храниться в каталоге C:\Public\Press (общий ресурс PressRepl).

Примечание Поскольку Вы создали изолированную DFS-ссылку, копирование (синхронизацию) файлов между папками придется осуществлять вручную. Для реплик изолированных DFS-ссылок службы тиражирования файлов недоступны.

1. В дереве консоли выберите ссылку News.
2. В меню Action (Действие) выберите команду New Replica (Создать реплику).
   Откроется диалоговое окно Add A New Replica (Добавить новую реплику).
3. В поле Send User To This Shared Folder (Переадресовать пользователя на эту общую папку) введите \\SERVER01\PressRepl. Заметьте: настроить политику репликации для данной реплики нельзя.
4. Щелкните кнопку OK.
   На правой панели появятся общие ресурсы \\SERVER01 \Press и \\SERVER01\Press-Repl.

► **Задание 5: обратитесь к изолированному корню DFS на Server01**

Используя командный файл с прилагаемого компакт-диска, скопируйте файлы в папки, на которые указывают созданные DFS-ссылки. Скопировав файлы, обратитесь к ним через Windows Explorer.

Внимание! Работа прилагаемого командного файла будет корректной, только если работают оба сервера, общие ресурсы созданы согласно приведенным инструкциям и на обоих компьютерах учетная запись Administrator имеет пароль password.

1. Вставьте прилагаемый компакт-диск в привод CD-ROM на ServerOl.
2. В окне My Computer (Мой компьютер) дважды щелкните значок привода CD-ROM.
3. Откройте папку \chapt05\ex1.

4. Щелкните файл exlcopy.bat и выберите в меню File (Файл) команду Open (Открыть).

   Откроется окно командной строки, которое закроется по завершении копирования файлов.

   Все оставшиеся этапы следует выполнять на Server02.

5. Чтобы обратиться к изолированному корню DFS на ServerOl, откройте папку My Network Places (Мое сетевое окружение) на Server02 и дважды щелкните значок Computers Near Me.

   Откроется окно Computers Near Me (Соседние компьютеры), отображающее все компьютеры рабочей группы.

6. Щелкните Server01 и выберите в меню File (Файл) команду Open (Открыть).

   Откроется окно, отображающее все общие ресурсы, корень DFS (Public) и прочие объекты компьютера ServerOl. Заметьте: папка Public выглядит так же, как и любой другой обший ресурс Server01.

7. Щелкните папку Public и выберите в меню File (Файл) команду Open (Открыть).

   В открывшемся окне Вы увидите четыре созданных ранее DFS-ссылки.

8. Откройте все ссылки и убедитесь, что соответствующие папки содержат файлы:

Папка	Файлы
ftp	dirmap.htm, dirmap.txt
Intranet	Q240126 - Best Practices for Using Sysprep with NTFS Volumes.htm
News	press.wri
Tech	DFSnew.doc, RFC 1777.txt

   Заметьте: в папке intranet будут и другие файлы, поскольку DFS-ссылка указывает на каталог, созданный при установке Windows 2000 Server.

9. Какая из папок ссылается на ресурс вне ServerOl?

10. Какая из папок ссылается на диск, подключенный к ранее пустому каталогу?

11. Выполняя данное упражнение, Вы создали реплику DFS-ссылки Press. Имя реплики - \\SERVER01\PressRepl. DFS-ссылка представляет общую папку PressRepl и находится в каталоге C:\Public\Press. Просмотрев содержимое данного каталога, Вы обнаружите, что он пуст. Однако, если просмотреть DFS-ссылку News, Вы увидите в соответствующей папке файл Press.wri. Почему DFS-реплика PressRepl пуста?

Совет Для проверки состояния DFS-ссылок и для просмотра содержимого ссылки вызовите оснастку Distributed File System (Распределенная файловая система DFS).

Резюме

DFS упрощает работу с папками, расположенными на разных компьютерах сети. Отдельная общая папка DFS (корень DFS) является точкой доступа для остальных разделяемых папок сети (DFS-ссылок). DFS организует общие папки разных компьютеров сети в единую логическую иерархическую файловую систему. DFS облегчает просмотр и администрирование сетевых ресурсов, сохраняя сетевые разрешения. На компьютере Windows 2000 Server можно сконфигурировать два вида корней DFS: изолированные и доменные. Изолированный корень хранит топологию DFS на отдельном компьютере и не обеспечивает отказоустойчивости при сбое компьютера, хранящего топологию DFS, или при отказе компьютеров, содержащих включенные в корень общие папки. Топология доменного корня содержится в хранилище Active Directory, а DFS-ссылки могут указывать на несколько идентичных общих папок, что обеспечивает отказоустойчивость. Кроме того, доменная DFS поддерживает DNS, множественные уровни дочерних томов, а также репликацию файлов. Для репликации данных в доменных корнях и ссылках применяется служба репликации файлов (FRS). Изменения DFS-ссылки в составе доменного корня DFS автоматически реплицируются для других членов реплики.

Занятие 2. Служба репликации файлов

FRS — служба репликации файлов в Windows 2000 Server — применяется для одновременного копирования и поддержки актуальности файлов на нескольких серверах и для репликации системного тома Windows 2000 (SYSVOL) на все контроллеры домена. FRS можно настроить и для репликации данных всех доменных корней DFS.

Изучив материал этого занятия, Вы сможете:

- ✓ рассказать, какие данные можно тиражировать, используя FRS;
- ✓ настроить тиражирование для доменных корней DFS;
- ✓ описать процесс тиражирования в службе Active Directory и в FRS.

Продолжительность занятия — около 25 минут.

Репликация посредством FRS

FRS автоматически устанавливается на все компьютеры Windows 2000 Server. На контроллерах домена она настраивается для автоматического запуска; на изолированных серверах и рядовых серверах домена FRS конфигурируется для запуска вручную. Хотя репликация Active Directory и служба FRS друг от друга не зависят, они совместно используют одну топологию, терминологию и методологию репликации. Фактически Active Directory с помощью FRS выполняет синхронизацию каталога между контроллерами домена.

В любом домене Windows 2000 есть один или несколько серверов — контроллеров домена. На каждом контроллере хранится полная копия хранилища Active Directory соответствующего домена; все домены участвуют в изменениях и обновлениях каталога.

В пределах сайта служба Active Directory автоматически создает кольцевую топологию для репликации данных между контроллерами одного домена. Топология определяет путь, по которому обновления каталога передаются между контроллерами до тех пор, пока их не получат все контроллеры.

Кольцевая структура гарантирует наличие не менее двух путей репликации между контроллерами; если один из контроллеров временно не работает, данные по-прежнему реплицируются на остальные контроллеры домена.

Служба Active Directory использует репликацию с несколькими хозяевами, когда ни один из контроллеров домена не является хозяином и все контроллеры равноправны.

Active Directory периодически анализирует топологию репликации сайта в целях обеспечения ее эффективности. При добавлении или удалении контроллера из сети или сайта служба Active Directory соответственно изменяет топологию.

Сайты и репликация

Сайт состоит из одной или нескольких IP-подсетей, определяющих группу компьютеров с надежным соединением. Рекомендуется объединять лишь подсети с быстрым и надежным каналом связи со скоростью не менее 512 кбит/с.

В Active Directory поддержка структуры домена и структуры сайта осуществляется отдельно. Домен может включать несколько сайтов, а сайт — несколько доменов или их части (рис. 5-5).

Рис. 5-5. Домен с одним сайтом, домен с несколькими сайтами и несколько сайтов с несколькими доменами

Существует два типа репликации; внутрисайтовая и межсайтовая.

Репликация внутри сайта

Ниже перечислены характеристики внутрисайтовой репликации:

- осуществляется между контроллерами домена в пределах сайта;
- реплицируемые данные не сжимаются;
- интервал репликации по умолчанию составляет 5 минут;
- репликация выполняется по запросу после получения уведомления.

Репликация между сайтами

Ниже перечислены характеристики межсайтовой репликации:

- осуществляется между контроллерами домена различных сайтов;
- администратор вправе задать интервал репликации (по умолчанию 5 минут);
- администратор может задать протокол, используемый при репликации;
- независимо от используемого протокола реплицируемые данные сжимаются;
- сжатие позволяет снизить трафик репликации на 88-90%.

Одним из недостатков межсайтовой репликации является отсутствие автоматической настройки — все параметры администратор определяет вручную.

Knowledge Consistency Checker

Процесс *проверки непротиворечивости знаний* (Knowledge Consistency Checker, KCC) генерирует в пределах сайта кольцевую топологию для репликации данных между контроллерами одного домена. Эта топология определяет путь, по которому обновления каталога будут передаваться между контроллерами до тех пор, пока все контроллеры домена не получат эти обновления.

Кольцевая структура гарантирует наличие не менее двух путей тиражирования между контроллерами; если один из контроллеров временно не работает, репликация продолжается на остальные контроллеры домена. Кроме того, кольцевая топология генерируется так, что обновление каталога передается от исходного контроллера к любому другому контроллеру домена, входящему в данный сайт, не более чем в три этапа.

KCC периодически анализирует топологию репликации сайта в целях обеспечения ее эффективности. При добавлении или удалении из сети контроллера или сайта KCC соответственно изменяет топологию.

Примечание Администратор вправе изменять топологию, включая перенастройку расписания межсайтовой репликации.

Уникальные порядковые номера

При изменении объекта каталога на контроллере домена в результате репликации данных с другого контроллера домена либо действий пользователя или администратора первый контроллер присваивает изменению *порядковый номер обновления* (Update Sequence Number, USN). Каждый контроллер домена использует собственные USN и присваивает их изменениям каталога по возрастающей.

При записи изменения в каталог контроллер домена вместе со свойством также записывает порядковый номер обновления.

Все контроллеры домена ведут таблицу USN, получаемых от других контроллеров; в таблице указывается наибольший USN, полученный от каждого из контроллеров. Контроллер домена периодически оповещает другие контроллеры о получении изменений и пересылает этим контроллерам свой текущий USN. Каждый контроллер, принимающий такое оповещение, проверяет в своей таблице USN последний уникальный порядковый номер, полученный от контроллера, отославшего оповещение; если какие-либо изменения не были получены, контроллер домена запросит их.

Применение USN не требует регистрации времени изменения и позволяет отказаться от синхронизации часов на контроллерах одного домена. Упрощается и восстановление системы при отказе. После сбоя контроллер домена повторно запускает тиражирование, опрашивая остальные контроллеры в поисках USN, старших его собственных. Так как при внесении изменений таблица USN обновляется автоматически, прерванные циклы репликации продолжаются с места сбоя, без потерь или дублирования обновлений.

Внедрение FRS

Включает несколько этапов: репликация SYSVOL, репликация доменных корней DFS, а также конфигурирование службы FRS для репликации между сайтами.

Репликация тома SYSVOL

Изменения каталога %systemroot%\SYSVOL любого контроллера домена автоматически реплицируются на остальные контроллеры в сайте. Хотя процесс и топология идентичны

репликации Active Directory, они не зависят от последнего. При добавлении, удалении или изменении содержимого папки %systemroot%\SYSVOL любого контроллера домена соответствующие изменения автоматически реплицируются на остальные контроллеры сайта.

Ниже приведена структура каталога по умолчанию:

- %systemroot%\SYSVOL\Sysvol*имя_домена*\Policies
- %systemroot%\SYSVOL\Sysvol*имя_домена*\Scripts

Любые файлы и каталоги, добавляемые в папку %systemroot%\ SYSVOL\Sysvol*имя_домена*, реплицируются автоматически.

Репликация отказоустойчивых томов DFS

Для репликации данных в DFS-ссылках уровня домена применяется служба FRS. Модификация DFS-ссылки из доменного корня DFS автоматически копируется другим членам реплики.

DFS и репликация файлов поддерживают следующие функции:

- репликация с несколькими хозяевами обеспечивает репликацию измененных файлов и списков управления доступом (ACL) после закрытия файла;
- возможность изменения файлов на любом члене реплики;
- репликация поддерживается лишь для разделов NTFS. Вы вправе публиковать прочие зеркальные общие ресурсы, однако реплицировать их придется вручную;
- журнал репликации;
- репликация основана на механизме удаленного вызова процедур (RPC);
- топология FRS соответствует топологии репликации Active Directory.

Процесс репликации DFS включает следующие этапы:

1. после закрытия файла отмечается, что он был изменен;
2. NTFS делает соответствующую запись в журнале NTFS Change Log;
3. FRS просматривает журнал NTFS на наличие изменений в DFS-ссылках;
4. FRS заносит запись в собственный журнал;
5. FRS создает промежуточный файл для процесса изменения;
6. FRS откладывает копирование модифицированной версии файла до запуска процесса репликации;
7. целевой сервер загружает промежуточный файл и вносит соответствующие изменения.

Добавление сервера с репликой корня DFS

Любой корень DFS или DFS-ссылка могут ссылаться на реплицированный набор общих ресурсов. Основываясь на топологии сайта, клиенты DFS автоматически выберут ближайшую реплику.

Чтобы добавить серверы с репликой корня в доменный корень DFS, в оснастке Distributed File System (Распределенная файловая система DFS) щелкните нужный корень правой кнопкой мыши, выберите в контекстном меню New (Создать), а затем — команду Root Replica (Корневая реплика). Укажите UNC-путь к серверу реплики и разделяемому ресурсу.

Включение репликации DFS

По умолчанию репликация DFS отключена. Для ее активизации щелкните в оснастке Distributed File System корень DFS или DFS-ссылку правой кнопкой мыши и выберите в контекстном меню команду Replication Policy (Политика репликации). Выделите все серверы набора реплик, которые будут задействованы в репликации FRS, и щелкните кнопку Enable. Серверы, не участвующие в репликации, придется синхронизировать вручную.

Настройка **службы FRS** для межсайтовой **репликации**

Межсайтовая репликация настраивается из оснастки Active Directory Sites and Services (Active Directory — сайты и службы). Настраивая параметры **FRS,** надо создать ссылку на новый сайт для межсайтового транспортного протокола, указанного в дереве консоли, затем щелкнуть ее правой кнопкой мыши и выбрать в контекстном меню команду Properties (Свойства), В открывшемся окне свойств можно задать необходимые параметры репликации между сайтами.

Резюме

FRS представляет собой автоматизированную службу репликации файлов Windows 2000 Server. Эта служба осуществляет копирование файлов одновременно на нескольких серверах. Существует два вида репликации: внутри сайта и между сайтами. Сайт представляет собой одну или несколько подсетей, объединяющих группу компьютеров по надежному соединению. Процесс проверки непротиворечивости знаний (KCC) автоматически генерирует в пределах сайта кольцевую топологию для репликации данных между контроллерами одного домена. Внедрение службы FRS состоит из нескольких этапов, включая репликации каталога SYSVOL, репликации доменных корней DFS и настройку FRS.

Закрепление материала

7 J Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Чем корень DFS отличается от диска, подключенного к пустой папке?

2. Выполняя упражнения, Вы заметили, что команды New Root Replica (Создать корневую реплику) и Replication Policy (Политика репликации) в оснастке Distirbuted File System были недоступны. Почему?

3. Почему **DFS** не предоставляет собственной системы зашиты?

4. Объясните роль процесса проверки согласованности знаний (KCC) в синхронизации хранилища Active Directory между контроллерами домена?

5. Какие данные реплицирует служба FRS?

ГЛАВА 6

Служба каталогов Active Directory

В этой главе

В главе 1 мы представили основные концепции Active Directory. А здесь мы обсудим такие возможности Active Directory, как масштабируемость, поддержка открытых стандартов, логическая и физическая структура хранилища Active Directory. В этой главе подробно описаны принципы функционирования и архитектуры Active Directory. Кроме того, рассмотрены особенности планирования и внедрения Active Directory в среде Microsoft Windows 2000. В заключение Вы узнаете об администрировании служб, реализованных в Windows 2000.

Прежде всего

Для изучения занятий этой главы потребуется:

- установить Windows 2000 Server на Server01 согласно инструкциям из упражнения 1 главы 2;
- обеспечить сетевое соединение с Server01 компьютера Computer 2, на котором также установлен Windows 2000 Server согласно инструкциям из упражнения 1 главы 3;
- установочный компакт-диск Windows 2000 Server.

Занятие 1. Обзор Active Directory

Active Directory — это служба каталогов Windows 2000 Server. Active Directory расширяет функциональность предыдущих служб каталогов Windows, включает новые возможности и обеспечивает безотказную работу л сетях любого размера: от одного сервера с несколькими сотнями объектов, до тысяч серверов с миллионами объектов. Множество новых функций Active Directory облегчают навигацию и управление большими объемами информации.

Изучив материал этого занятия, Вы сможете:

- ✓ описать принципы работы и архитектуру Active Directory.

Продолжительность занятия — около 40 минут.

Введение в Active Directory

Полностью интегрированная в Windows 2000 Server, служба Active Directory обеспечивает иерархическое представление объектов. Она расширяема, масштабируема и обладает распределенной системой безопасности. Active Directory позволяет администраторам, разработчикам и конечным пользователям получить доступ к службе каталога, прозрачно интегрированной как в глобальную, так и корпоративную среду. Active Directory — важная часть распределенных систем и позволяет конечным пользователям и администраторам обращаться к службе каталогов как источнику информации и решать с ее помощью административные задачи.

Active Directory объединяет концепцию пространства имен Интернета со службой каталога ОС. *Пространство имен* (namespace) — это структурированная совокупность данных, в которой для символического представления информации применяются имена; порядок создания и использования этих имен регулируется правилами именования. Объединение концепции пространства имен и службы каталогов позволяет унифицированно управлять пространствами имен в разнородных программных и аппаратных средах корпоративных сетей. Основным протоколом в Active Directory является LDAP, способный взаимодействовать с различными ОС, включающими независимые пространства имен. Протокол LDAP позволяет управлять каталогами других приложений, а также каталогами сетевых ОС, что упрощает администрирование и снижает стоимость обслуживания множества пространств имен.

Active Directory не является каталогом X.500 — роль протокола доступа играет LDAP, поддерживается и информационная модель X.500, но без свойственной ей избыточности. Этим достигается высокий уровень совместимости с существующими разнородными сетями.

Примечание О протоколе X.500 см. также документ \chapt01\ articles\RFC 1777.txt. на прилагаемом компакт-диске.

Active Directory позволяет централизованно администрировать все опубликованные ресурсы: файлы, периферийные устройства, хост-соединения, базы данных, доступ к Интернету, учетные записи пользователей, службы и другие объекты. Active Directory применяет в качестве службы поиска реализованную в Интернете *систему доменных имен* (Domain Name System, DNS), упорядочивающую объекты в доменах в иерархию организационных подразделений (ОП), и позволяет объединить несколько доменов в древовидную

структуру. Это также помогает упростить администрирование за счет отказа от иерархии основной/резервный контроллер домена, применявшейся в Windows NT Server, поскольку в Active Directory все контроллеры равноправны. Изменения, внесенные на любом контроллере домена, будут скопированы на все остальные контроллеры.

Примечание О возможностях, принципах работы и архитектуре Active Directory см. также статьи Managing the Active Directory.doc, Active_Directory_Technical_Summary.doc и Active_Directory_ DS_Strategy.doc в папке \chapt06\articles на прилагаемом компакт-диске.

Концепция Active Directory

Здесь рассматриваются некоторые новые принципы, веденные в Active Directory: расширяемая схема, глобальный каталог, пространство имен и правила именования.

Расширяемая схема

Схема содержит формальное описание содержания и структуры хранилища Active Directory, включая все атрибуты, классы и свойства классов. Для каждого класса объектов *схема* (schema) определяет, какими атрибутами должен обладать экземпляр класса, какие дополнительные атрибуты он может иметь и какой класс объектов может являться предком текущего класса.

При установке Active Directory на первый контроллер домена в сети создается стандартная схема, содержащая определения наиболее часто используемых объектов и их свойств, таких как пользователи, компьютеры, принтеры и группы. Стандартная схема также содержит определения собственных объектов и свойств Active Directory.

Схема Active Directory расширяема, т. е. Вы вправе определять новые типы объектов каталогов и их атрибуты, в том числе и новые атрибуты для существующих объектов. Схема внедряется и хранится вместе с Active Directory (в глобальном каталоге) и обновляется динамически. Таким образом, приложение способно дополнять схему новыми атрибутами и классами и сразу задействовать эти расширения.

Расширение схемы Active Directory

Эта операция требует углубленных знаний и должна проводится опытными программистами и системными администраторами. Перед внесением изменений в схему изучите соответствующие темы в справочной системе Windows 2000, а также руководство *Active Directory Programmer's Guide* по адресу http://msdn.microsoft.com/developer/windows2000/adsi/actdirguide.asp. Если Вы не найдете данный документ по указанному адресу, загляните на узел http://msdn.microsoft.com. *Active Directory Programmer's Guide* включает подробное описание всех способов расширения схемы Active Directory, а также примеры сценариев и исходных текстов программ.

Внимание! Последствия расширения схемы затронут всю сеть, поэтому рекомендуется изменять схему программно и только при крайней необходимости. Некорректная модификация схемы нарушит работу Windows 2000 Server, а возможно и сети.

Глобальный каталог

Это центральное хранилище информации об объектах в дереве доменов (совокупности доменов, формирующих его иерархию) или в лесе (совокупности деревьев доменов из различных иерархий). Active Directory генерирует содержание *глобального каталога* (global

catalog) из доменов в составе каталога путем обычного процесса репликации. Система репликации Active Directory автоматически создает глобальный каталог и определяет топологию репликации.

Глобальный каталог (ГК) является как службой, так и физическим хранилищем реплики части атрибутов всех объектов Active Directory. Процесс частичной репликации позволяет находить большинство сведений прямо в ГК, без опроса исходного домена. По умолчанию в ГК хранятся атрибуты, наиболее часто указываемые в операциях поиска (например имя и фамилия пользователя, его регистрационное имя и т. п.), а также сведения, необходимые для обнаружения полной реплики объекта. Следовательно, ГК позволяет найти объект в любом месте сети, даже не реплицируя информацию между контроллерами домена.

Примечание Для выбора атрибутов, реплицируемых в ГК, применяется оснастка Active Directory Schema (Схема Active Directory) — см. каталог %systemroot%\system32, файл Schmmgmt.msc. Будьте осторожны! Только опытные программисты и высококвалифицированные администраторы, четко представляющие, что такое схема и как она функционирует, могут пользоваться этим инструментом.

При установке Active Directory на первый контроллер домена, он по умолчанию становится сервером ГК — на нем хранится его копия. В зависимости от размеров сети сервер ГК должен быть достаточно мощным, чтобы поддерживать от нескольких сотен тысяч до миллиона объектов с перспективой дальнейшего роста их количества,

Оснастка Active Directory Sites and Services (Active Directory — сайты и службы) позволяет сконфигурировать дополнительные контроллеры домена в качестве серверов ГК. Выбирая сервер ГК, надо учесть, справится ли сеть с трафиком репликации и запросов — чем больше таких серверов, тем он выше. Впрочем, дополнительные серверы позволят ускорить время отклика на запросы пользователей. Рекомендуется, чтобы каждый крупный сайт предприятия имел собственный сервер ГК.

Пространство имен

Как и любая служба каталогов, Active Directory в первую очередь является пространством имен. *Пространство имен* (namespace) — это любая ограниченная область, где возможно разрешение имени (рис. 6-1). *Разрешение имени* (name resolution) — это процесс сопоставления имени некоему объекту или информации, которую оно представляет, Пространство имен Active Directory основано на схеме именования DNS, обеспечивающей взаимодействие с Интернетом.

Применение общего пространства имен позволяет централизованно управлять многочисленными аппаратными и программными средами сети. Существует два типа пространств имен:

- *связное* (contiguous) — имя дочернего объекта в иерархии всегда содержит имя родительского домена, например, дерево — связное пространство имен;
- *раздельное* (disjointed) — имена родительского объекта и его дочернего объекта напрямую не связаны, например, лес — раздельное пространство имен.

Правила именования

Каждый объект в хранилище Active Directory идентифицируется по имени. В Active Directory применяются разные правила именования: *составные имена* (distinguished name, DN), *относительные составные имена* (relative distinguished name, RDN), *глобально уникальные идентификаторы* (globally unique identifier, GUID) и *основные имена пользователей* (user

principal name, UPN). Active Directory является LDAP-совместимой службой каталога, т. е. все обращения к объектам в каталогах осуществляются по протоколу LDAP.

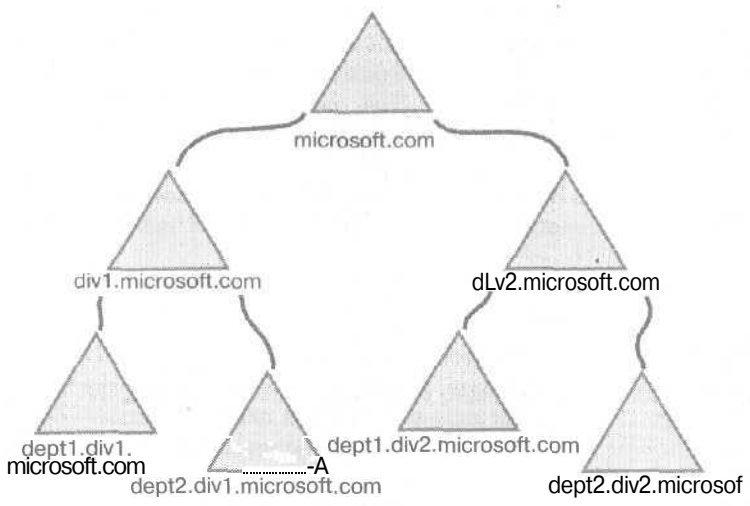


Рис. 6-1. Пример диаграммы пространства имен домена

Составное имя

Объекты размещаются в доменах Active Directory согласно иерархическому пути, включающему метки доменного имени Active Directory и всех уровней контейнерных объектов. Каждый объект в хранилище Active Directory имеет составное имя. Оно уникально идентифицирует объект и содержит информацию для клиента, достаточную для извлечения объекта из каталога. DN включает имя домена, содержащего объект, и полный путь к объекту по иерархии контейнеров.

Следующее DN идентифицирует объект-пользователя James Smith в домене microsoft .com:

```
DC=COM/DC=Microsoft/CN=Users/CN=James Smith
```

Разделители и значения, использованные в DN для James Smith, таковы:

LDAP- разделитель	Значение	Представляет
DC	**COM**	**Компонент домена**
DC	**Microsoft**	**Компонент домена**
CN	**Users**	**Общее имя**
CN	**James Smith**	**Общее имя**

Заметьте: в оснастке не отображаются сокращения LDAP (O=, DC=, CN=). Они приведены здесь лишь для иллюстрации того, как LDAP распознает составные части DN. Некоторые из сокращений, описанных в RFC-документах, например O= для наименования организации и C= для страны, в Active Directory не применяются, хотя и распознаются протоколом LDAP.

Примечание О составных именах см, также документ \chapt06\artícles\ rfc1779.txt на прилагаемом компакт-диске.

Относительное составное имя

В Active Directory можно найти объект, даже не зная его точного DN или если это имя было изменено. Поиск можно вести по атрибутам объекта, один из которых — относительное составное имя, часть полного DN. В предыдущем примере RDN для объекта-пользователя James Smith будет CN=James Smith, а для родительского объекта — CN=Users.

Active Directory позволяет копировать RDN объектов, однако в рамках одного организационного подразделения такие имена должны быть уникальны. Например, если в ОП Users есть учетная запись пользователя James Smith, добавить в то же ОП запись одноименного пользователя нельзя. Однако если ОП Users содержит два меньших ОП, например Managers и Sales, то в обоих разрешено создать учетную запись James Smith, поскольку каждая будет иметь уникальное DN.

Глобально уникальный идентификатор

Помимо DN, каждый объект в хранилище Active Directory обладает глобально уникальным идентификатором — 128-разрядным номером, назначенным агентом DSA при создании объекта. GUID не изменяется даже после перемещения или переименования объекта. Приложения могут хранить GUID объекта и гарантированно находить объект независимо от его текущего DN.

В Windows NT ресурсы домена были связаны с *идентификатором безопасности* (security identifier, SID), формируемом внутри домена, т. е, SID был уникален только в рамках домена. GUID уникален во всех доменах, причем его уникальность сохраняется при перемещении объектов из одного домена в другой.

GUID хранится в атрибуте objectGUID, которым обладает каждый объект. Этот атрибут защищен от изменения и удаления. При сохранении ссылки на объект Active Directory во внешнем хранилище (например в базе данных Microsoft SQL Server) следует использовать значение objectGUID (рис. 6-2).

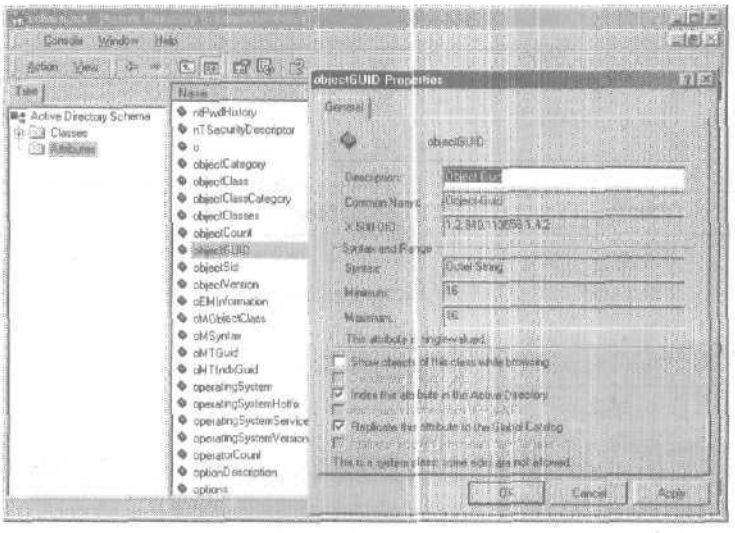


Рис. 6-2, Атрибут objectGUID в оснастке Active Directory Schema Management (Схема Active Directory)

Основное имя пользователя

Это дружественное имя, которое короче DN и легче для запоминания. Основное имя пользователя состоит из сокращенного имени, представляющего пользователя, и, как правило, DNS-имени домена, в котором находится объект USER. Формат основного имени таков: имя пользователя, символ @, суффикс основного имени пользователя. Например, пользователь James Smith в microsoft.com мог бы иметь основное имя вида username@microsoft.com. UPN не зависит от DN объекта-пользователя, поэтому объект User разрешается перемещать или переименовывать, не изменяя регистрационного имени пользователя.

Архитектура Active Directory

Active Directory составляют несколько основных архитектурных компонентов: схема, модели данных, безопасности и администрирования.

Модель данных

Унаследована от модели данных X.500. Каталог содержит объекты, представляюшие различные компоненты сети. Каждый объект представлен атрибутами. Совокупность объектов, допустимых для хранения в каталоге, определяется схемой.

Схема

Реализована как набор экземпляров классов объектов, хранимых в каталоге. Схема может обновляться динамически, т. е. приложение вправе добавить в схему новые атрибуты и классы и сразу использовать эти расширения. Схема обновляется путем создания или изменения хранимых в каталоге объектов схемы. Как и все объекты хранилища Active Directory, объекты схемы защищены *списками управления доступом* (access control list, ACL), поэтому изменять схему разрешено только правомочным пользователям.

Модель безопасности

Каталог — полноценная составляющая инфраструктуры безопасности Windows 2000. ACL защищает все объекты в хранилище Active Directory. Средства авторизации доступа Windows 2000 применяют ACL для разрешения доступа к объектам или атрибутам в хранилище Active Directory.

Модель администрирования

Active Directory администрируют только авторизованные пользователи. Администратор вправе предоставить пользователю некий стандартный набор разрешений для выполнения только определенных действий над указанной совокупностью экземпляров или классов объектов в конкретном поддереве каталога, т. е. делегировать административные полномочия. Это позволяет четко контролировать распределение полномочий, не предоставляя каждому отдельному пользователю конкретные разрешения.

Доступ к Active Directory

Доступ к Active Directory осуществляется по сетевым протоколам, определяющим форматы передаваемых сообщений и способы взаимодействия клиента с сервером. Доступ к этим протоколам предоставляют *интерфейсы прикладного программирования* (application programming interface, API).

Протоколы, поддерживаемые Active Directory

- **LDAP** — основной протокол Active Directory, поддерживается LDAP 2 и 3;
- **MAPI-RPC** — Active Directory поддерживает интерфейсы *удаленного вызова процедур* (remote procedure call, RPC) через интерфейсы MAPI;

- X.500 — информационная модель Active Directory унаследована от модели X.500. В стандарте X.500 определено несколько сетевых протоколов, не реализованных в Active Directory отчасти из-за их зависимости от модели OSI:
  - Directory Access Protocol (DAP);
  - Directory System Protocol (DSP);
  - Directory Information Shadowing Protocol (DISP);
  - Directory Operational Binding Management Protocol (DOP).

Интерфейсы прикладного программирования

Служба Active Directory обладает мощными, гибкими и простыми в работе API. Богатый набор API для службы каталога способствует разработке использующих ее приложений и инструментов.

Интерфейсы Active Directory

В помощь разработчикам приложений, взаимодействующих с Active Directory и другими LDAP-совместимыми каталогами, в Microsoft был создан Active Directory Service Interface (ADSI) — набор расширяемых интерфейсов для разработки приложений, взаимодействующих *с:*

- Active Directory;
- любым каталогом на базе LDAP;
- другими службами каталогов, включая Novell Directory Services (NDS).

ADSI — это часть Open Directory Services Interfaces (ODSI) и Windows Open Services Architecture (WOSA). Объекты ADSI доступны для служб каталогов Windows NT 4.0, Novell NetWare 3.x и 4.x, Active Directory и любых служб каталогов, поддерживающих LDAP.

ADSI включает функции служб каталогов, позволяющие единообразно управлять ресурсами в различных сетях. Это упрощает разработку приложений для распределенных систем и их администрирование. ADSI позволяет разработчикам и администраторам перечислять ресурсы и управлять ими независимо от сетевой среды, содержащей ресурс. Так что ADS1 облегчает выполнение общих административных задач: регистрацию новых пользователей, управление работой принтеров и определение местоположения ресурса в распределенной среде.

Объекты ADSI предназначены для удовлетворения потребностей:

- разработчиков — они используют ADSI совместно с компилируемым языком, например C++, хотя для создания прототипа приложения можно задействовать и Microsoft Visual Basic; ADSI позволяет создать приложение, управляющее многочисленными каталогами, сетевой печатью, резервным копированием баз данных и т. п.;
- системных администраторов — они обращаются к ADSI через язык сценариев, например Microsoft Visual Basic, хотя для повышения производительности можно использовать и C/C++; так, администратор мог бы написать сценарий для добавления в систему 100 новых пользователей и включения их в определенную группу;
- пользователей — они, как и системщики, обращаются к ADSI на языке сценариев; так, пользователь может написать сценарий для поиска всех заданий печати в группе очередей печати и отображения состояния каждого задания.

*API-интерфейс **LDAP C***

Самое низкоуровневое решение для разработчиков приложений, поддерживающих различные типы клиентов. LDAP-приложения взаимодействуют с Active Directory после незначительной модификации или вообще без изменений для поддержки собственных типов объектов Active Directory. Разработчикам LDAP-приложений выгодно перейти на интерфейс ADSI, поскольку он поддерживает любые LDAP-совместимые службы каталогов.

Windows ***Messaging API***

Active Directory поддерживает старые MAPI-приложения. Впрочем, в основе новых приложений для доступа к службе каталога лучше использовать ADSI.

Виртуальные контейнеры

Active Directory поддерживает виртуальные контейнеры, обеспечивающие прозрачный доступ к любому каталогу, основанному на LDAP. Виртуальный контейнер реализуется посредством информации о местоположении объектов из хранилища Active Directory. Эта информация определяет, в каком месте Active Directory должен быть представлен внешний каталог, включает DNS-имя сервера, хранящего копию фактического каталога, а также DN, с которого надо начинать поиск во внешней службе каталогов.

Архитектура службы каталогов

В многоуровневой архитектуре Active Directory каждый уровень соответствует серверному процессу, предоставляющему службы каталога клиентским приложениям (рис. 6-3). Архитектура Active Directory включает три уровня служб, несколько интерфейсов и протоколов. Уровни служб (системный агент каталога, уровень базы данных и расширяемое ядро хранилища) обрабатывают данные, необходимые для поиска записей в базе данных (БД) каталога. Над уровнями служб в этой архитектуре расположены протоколы и интерфейсы, обеспечивающие взаимодействие клиентов со службой каталогов.

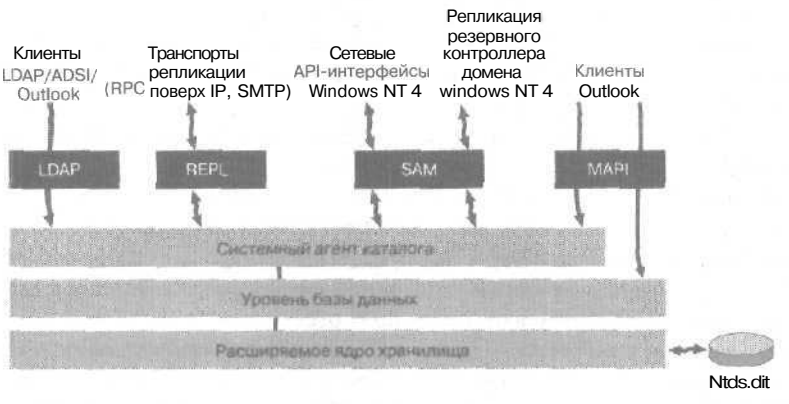


Рис. 6-3. Архитектура Active Directory

Active Directory включает следующие ключевые компоненты.

- **Системный агент каталога (Directory System Agent, DSA)** формирует иерархию на основе хранимых в каталоге сведений об отношениях родитель — потомок; предоставляет API-интерфейсы для выполнения запросов доступа к каталогу.
- **Уровень базы данных** абстрагирует приложения от БД; приложения никогда не обращаются напрямую к БД, только через уровень БД.
- **Расширяемое ядро хранилища (Extensible Storage Engine, ESE)** взаимодействует с индивидуальными записями в хранилище данных каталога на основе RDN объекта.
- **Хранилище данных (файл базы данных Ntds.dit)** обрабатывается только ядром хранилища; администрирование этого файла осуществляется из утилиты Ntdsutil,

Примечание При установке Windows 2000 Server исполняемый файл этой утилиты, Ntdsutil.exe, размещается в каталоге %systemroot%\system32.

Интерфейсы

Клиент получает доступ к Active Directory за счет механизмов, поддерживаемых DSA:

Интерфейс	Описание
MAPI	Устаревшие клиенты MAPI, например клиент Microsoft Out-look, для обмена сообщениями подключаются к DSA посредством MAPI RPC-интерфейса поставщика адресной книги.
LDAP	Предоставляет интерфейс для взаимодействия LDAP-клиентов с ADSI, что позволяет разрабатывать приложения, способные общаться с Active Directory. Клиенты, поддерживающие протокол LDAP, используют его для подключения к DSA. Active Directory поддерживает LDAP версий 2 и 3. Клиенты Windows 2000 и Windows 9x, на которых установлены клиентские компоненты Active Directory, применяют для подключения к DSA протокол LDAP версии 3. Интерфейс ADSI является средством абстрагирования от API-интерфейса протокола LDAP, однако Active Directory использует только LDAP.
REPL	Используется службой репликации для репликации сведений из Active Directory через RPC поверх протоколов IP или SMTP из стека протоколов TCP/IP. SMTP применяется только для межсайтовой репликации; RPC поверх IP используется как для внутри-, так и для межсайтовой репликации.
SAM	Обеспечивает низкоуровневую совместимость для связи доменов Windows 2000 и Windows NT 4.0. Клиенты, использующие Windows NT 4.0 или более ранние версии этой ОС, через интерфейс SAM соединяются с DSA. Репликация информации с резервных контроллеров доменов в домен смешанного режима также осуществляется через интерфейс SAM.

Системный агент каталога

Системный агент каталога (Directory System Agent, DSA) — это процесс, управляющий физическим хранилищем каталога. Для подключения к DSA клиенты применяют один из поддерживаемых интерфейсов, а затем ищут в каталоге разрешенные для модификации объекты и их атрибуты. DSA изолирует клиент от формата физического хранилища данных каталога, что обеспечивает удобный доступ и защиту системы.

DSA предоставляет доступ к хранилищу — файлу БД, содержащему информацию о каталогах на жестком диске. Уровень DSA предоставляет интерфейсы для поддержки следующего набора операций ядра.

Идентификация объекта

Каждый объект в хранилище Active Directory имеет постоянный GUID, связанный с символьным представлением имени объекта. Имя разрешается изменять, поэтому все постоянные ссылки на объект сохраняются с применением GUID. Имя используется для навигации по иерархии и для отображения объекта. DSA обеспечивает взаимосвязь GUID и объекта при изменении его составного имени.

Обработка транзакций

Транзакции обрабатываются автоматически. Запрос записи выполняется с фиксацией всех изменений либо отменяется и не оказывает никакого влияния, Транзакции синхронно регистрируются в файле журнала, а затем и в БД.

Согласование обновлений схемы

Копирование и синхронизация информации каталога называется репликацией *с несколькими хозяевами* (multimaster replication). В системах с несколькими хозяевами изменение

объекта схемы в одной реплике может вызвать конфликт с существующими объектами в той же реплике, и с объектами в других. Схема является формальным определением каждого класса объектов, которые могут быть созданы в каталоге, атрибутов каждого класса объектов и допустимых родителей для каждого класса. В Windows 2000 изменение схемы выполняется как *операция с одним хозяином* (single-master operation), т. е. все изменения, внесенные на хозяине, будут отражены во всех репликах. При обработке реплицированных обновлений схема не проверяется. Основной целью является согласование реплик объекта друг с другом; согласование с изменяющейся схемой — задача второстепенная.

Контроль доступа

DSA следит за соблюдением ограничений безопасности при доступе к каталогу. Уровень DSA получает идентификаторы безопасности из маркера доступа.

Поддержка репликации

DSA включает средства для уведомления о репликации. Для корректной работы службы каталогов все обновления объектов должны быть соответствующим образом обработаны.

Ссылки

DSA обрабатывает информацию об иерархической структуре каталога, которую получает от уровня БД. DSA отвечает за перекрестные ссылки доменных объектов Active Directory в дереве иерархии, а также за ссылки на другие доменные иерархии.

Уровень базы данных

Обеспечивает объектное представление информации БД путем применения семантики схемы к записям БД и изолирования верхних уровней службы каталога от исходной СУБД. Уровень БД является скрытым внутренним интерфейсом. Все обращения к базе данных проходят через уровень БД.

Active Directory предоставляет иерархическое пространство имен. Каждый объект однозначно идентифицируется в БД по RDN. Это имя и цепочка имен последующих родительских объектов формирует DN объекта. В БД для каждого объекта хранится RDN и ссылка на родительский объект. Уровень БД следует этим родительским ссылками и объединяет последующие RDN для формирования DN объекта.

Основной функцией уровня БД является перевод каждого разлисоставного имени в целое число — тег, применяемый для всех внутренних операций доступа. Уровень БД гарантирует уникальность тега DN для каждой записи в базе.

Все данные, описывающие объект, содержатся в виде набора атрибутов, хранимого как поля записи в БД. Уровень БД отвечает за создание, извлечение и удаление индивидуальных записей, полей записей и значений полей. Для этого применяется кэш схемы (резидентная структура в DSA), содержащий информацию о необходимых атрибутах.

Расширяемое ядро хранилища

Службы Active Directory реализованы поверх диспетчера таблиц ISAM. Более ранняя версия этого диспетчера таблиц, JET, применялась в Microsoft Exchange Server 5.5, службе репликации файлов (FRS), редакторе конфигурации безопасности, сервере сертификатов, службе WINS и в других компонентах Windows. В Windows 2000 действует новая улучшенная версия JET — Extensible Storage Engine (ESE).

ESE (Esent.dll) реализует транзакционную БД, применяющую файлы журнала для подтверждения корректного выполнения транзакций. Так что служба каталога использует как файлы данных (Ntds.dit), так и файлы журнала. По умолчанию файлы Esent.dll и Ntds.dit хранятся в каталоге %systemroot%\system32.

ESE отвечает за хранение всех объектов Active Directory и поддерживает БД объемом до 16 Тб, теоретически способную содержать несколько миллионов объектов для каждого домена. ESE удовлетворяет потребности Active Directory по хранению информации:

- выполняет операции обновления в виде транзакций для поддержания устойчивости и целостности системы на случай системных сбоев;
- эффективно обрабатывает разреженные поля, в которых многим свойствам не присвоены значения.

При установке Active Directory создается стандартная схема, определяющая все необходимые и допустимые атрибуты для данного объекта, ESE оставляет место только для используемого пространства, т. е. для назначенных объекту атрибутов, а не для всех возможных атрибутов. Например, если у объекта в схеме определено 50 атрибутов и Вы регистрируете пользователя только с четырьмя, выделяется пространство для хранения только этих атрибутов. Если в дальнейшем будут добавлены новые атрибуты, для их размещения будет выделен больший объем.

ESE также позволяет хранить атрибуты, имеющие множество значений, например, **БД** может содержать несколько телефонных номеров одного пользователя — создавать отдельный атрибут для каждого номера не требуется.

Службы Active Directory являются функциональным надмножеством службы каталогов Exchange Server и обладают дополнительными возможностями, включая безопасное переименование объектов, динамически расширяемую схему, репликацию и разрешение конфликтов на уровне атрибутов. ESE реализует функции поиска и извлечения информации из исходной **БД.**

Резюме

Службы Active Directory обеспечивают иерархическое представление содержания каталога, расширяемость, масштабируемость и соблюдение правил безопасности. Active Directory объединяет концепцию пространства имен Интернета со службой каталога ОС. LDAP — основной протокол Active Directory — позволяет централизованно работать с каталогами различных ОС, объединяя множество пространств имен. Схема содержит формальное описание содержания и структуры хранилища Active Directory, включая все атрибуты, классы и свойства классов. Глобальный каталог — центральное хранилище информации об объектах в дереве или лесе — выполняет роль службы и физического хранилища, содержащего реплику ряда атрибутов каждого объекта в хранилище Active Directory. Как и все службы каталога, Active Directory — это прежде всего пространство имен; каждый объект в хранилище Active Directory идентифицируется по имени. Структура Active Directory включает несколько основных компонентов: схему, модели данных, безопасности и администрирования. Доступ к Active Directory осуществляется по сетевым протоколам, определяющим форматы сообщений и порядок взаимодействия клиентов с сервером. Архитектура Active Directory состоит из трех уровней, нескольких интерфейсов и протоколов, совместно предоставляющих службы каталога.

Занятие 2. Планирование внедрения Active Directory

Перед реализацией сетевой среды на базе Windows 2000 Вы должны решить, как внедрить Active Directory. При планировании нужно учесть структуру и деятельность предприятия: физическое размещение офисов, возможность расширения и реорганизации и порядок доступа к сетевым ресурсам. Сначала планируется пространство имен DNS, включая иерархию домена, глобальный каталог, доверительные отношения и репликацию. Кроме того, пространство имен включает организационные подразделения (ОП), структуру которых также следует учесть на этапе планирования, В одиночном домене объекты пользователей и ресурсов можно упорядочить в иерархию ОП для отражения структуры компании. Надо спланировать и границы сайтов — это упростит управление репликацией и сократит трафик регистрационных данных пользователей между подразделениями.

Изучив материал этого занятия, Вы сможете:

- ✓ планировать пространство имен, сайты и организационные подразделения при подготовке к внедрению Active Directory.

Продолжительность занятия — около 75 минут.

Планирование пространства имен

Подобно DNS, в основе пространства имен Active Directory лежит полное имя домена высшего уровня информационной системы предприятия, состоящей из доменов Windows 2000, контроллеров доменов, ОП, доверительных отношений и деревьев доменов. Кроме того, важно сразу решить, будут ли одинаковы внутреннее (защищенное брандмауэром) и внешнее (за его пределами) пространство имен. Иначе говоря, будет ли пространство имен Active Directory соответствовать пространству имен DNS (как правило, имени домена в Интернете), которое, возможно, уже определено для Вашей организации?

Допустим, внешнее пространство имен DNS организации — microsoft.com. Вы можете использовать пространство имен Active Directory, соответствующее microsoft.com, или выбрать другое внутреннее пространство имен. Каждый вариант имеет свои плюсы и минусы.

Примечание Это не значит, что DNS — исключительно внешнее пространство имен. Просто если пространства имен разделены, Active Directory будет администрироваться отдельно от внешнего пространства имен.

Внутреннее и внешнее пространства имен

Существует два варианта разработки пространства имен Active Directory: оно может соответствовать либо отличаться от имеющегося внешнего пространства имен DNS.

В этом разделе рассматриваются оба варианта реализации пространства имен. Первый сценарий подразумевает, что внутреннее и внешнее пространства имен одинаковы, т. е. названия доменов высшего уровня идентичны по обе стороны брандмауэра — пользователи корпоративной интрасети и пользователи Интернета видят имя microsoft.com. Во втором случае внутреннее и внешнее пространства имен различны, т. е. имя домена высшего уровня в пределах брандмауэра отличается от высшего зарегистрированного имени домена DNS, видимого из Интернета. Внутреннее пространство имен будет expedia.com, а внешнее — microsoft.com.

Сценарий 1. Внутреннее и внешнее пространства имен идентичны

По этому сценарию организация использует одно и то же имя для внешнего и внутреннего пространств имен. Например, имя microsoft.com будет применяться для доступа к ресурсам как изнутри организации, так и из Интернета. Для реализации этого сценария надо соблюсти следующие условия:

- клиенты внутренней сети должны иметь доступ к внутреннему и внешнему серверам (по обе стороны брандмауэра);
- клиенты, обращающиеся к ресурсам извне, не должны иметь доступ к внутренним ресурсам организации или разрешению имен.

Для реализации этого сценария необходимы две раздельные зоны DNS. Одна — за пределами брандмауэра — будет обеспечивать разрешение имен только для общедоступных ресурсов. В результате внутренние ресурсы компании будут недосягаемы для внешних клиентов.

Минус этой конфигурации — предоставление доступа внутренним клиентам к общедоступным ресурсам путем разрешения имен. Одно из решений — создание дубликата внешней зоны на внутренней зоне DNS, что позволит внутренним клиентам разрешать ресурсы. При использовании прокси-сервера прокси-клиент надо настроить так, чтобы он обращался к microsoft.com как к внутреннему ресурсу.

Преимущества

- Имя дерева, microsoft.com, согласовано в частной сети и Интернете.
- Появляется возможность унифицировать вход в систему — для этого пользователи локальной сети и Интернета смогут применять одно и то же имя, например username@microsoft.com будет служить как регистрационное имя и как идентификатор электронной почты.

Недостатки

- Усложняется конфигурация — при настройке прокси-клиентов надо учесть, что внутренние и внешние ресурсы отличаются.
- Придется следить, чтобы внутренние ресурсы случайно не стали общедоступными.
- Вдвое усложняется управление ресурсами — например, придется дублировать записи зоны для внутреннего и внешнего разрешения имен.
- Даже если пространство имен одно и то же, внутренние и внешние ресурсы будут представляться пользователям по-разному.

Сценарий 2. Внутреннее и внешнее пространства имен различаются

По разные стороны брандмауэра — внутри и вне корпоративной сети — применяются разные имена. Например, пользователи Интернета будут видеть имя microsoft.com, а интрасети — expedia.com. Оба этих пространства имен должны быть зарегистрированы в DNS Интернета во избежание дублирования внутреннего имени в другой общей сети. Если внутреннее имя не зарезервировано и используется другой организацией, внутренние клиенты не отличат внутреннее имя от чужого публично зарегистрированного пространства имен DNS.

Будут установлены две зоны: одна будет отвечать за разрешение имен в пространстве microsoft.com, а другая — в пространстве expedia.com. В результате клиенты смогут четко различать внутренние и внешние ресурсы.

Преимущества

- Четкая разница между внутренними и внешними ресурсами за счет применения различных доменных имен.
- Упрощается администрирование.

- Упрощается настройка прокси-клиентов, поскольку списки исключения при опознавании внешних ресурсов должны будут содержать только expedia.com.

Недостатки

- Регистрационные **имена отличаются от имен электронной** почты. **Например,** если кто-**нибудь** входит **под именем** username@microsoft.com, **то адрес его электронной почты** будет username@expedia.com, **что** неудобно.
- В DNS Интернета придется зарегистрировать больше имен.

Совет В этом сценарии имена входа в систему различны по умолчанию. Администратор с помощью Microsoft Management Console (MMC) может изменить свойства UPN-суффикса пользователей так, чтобы имя пользователя для входа в систему совпадало с его электронным адресом.

Выбор архитектуры пространства имен

Выбрав модель взаимодействия внутреннего и внешнего пространств имен, надо учесть и другие факторы, например объем трафика репликации по ГВС и потенциальные изменения структуры предприятия. Помимо возможности создания леса в Windows 2000, администраторы должны быть готовы оперативно корректировать архитектуру пространства имен с минимальными издержками и без остановки работы сети. Цель — получить масштабируемую архитектуру, способную адаптироваться к изменениям, обеспечивающую непрерывный доступ к внутренним и внешним ресурсам и защиту данных.

Архитектура пространства имен должна отражать структуру предприятия и одновременно обеспечивать степень административной детализации, необходимую для эффективного управления корпоративной и глобальной сетью посредством Active Directory.

Соблюсти эти условия позволяет наличие трех уровней доменов:

- **корневой домен;**
- домен **первого уровня;**
- **домен второго уровня.**

Эта структура обеспечивает гранулярную топологию репликации и позволяет при необходимости ограничить полномочия нижестоящих администраторов.

Корневой домен

Это первый домен пространства имен, например expedia.com. *Корневой домен* (root domain) в Active Directory определяет пространство имен компании. Все внутренние домены являются частью этого домена, создавая непрерывное связное пространство имен в виде дерева доменов. Кроме того, серверы, содержащие корень пространства, скрыты за брандмауэром и, следовательно, не будут видимы из Интернета.

Домены первого уровня

Этот уровень модели отвечает за создание доменных имен, которые не изменяются даже при внутренней реорганизации предприятия. Простейший вариант — давать названия таким доменам, исходя из географических или политических границ, например noamer.expedia.com или europe.microsoft.com. Это также поможет сократить трафик репликации, поскольку сведения о пользователе в Северной Америке не нужно размещать на сервере Active Directory в Европе. Впрочем, серверы глобального каталога позволят найти ресурсы в Европе даже пользователю из Северной Америки.

Доверительные отношения между корневым доменом и всеми доменами первого уровня делают ресурсы доступными для всех ветвей дерева доменов. Следовательно, пользователь в noamer.expedia.com, может получить доступ к ресурсу в europe.microsoft.com.

Доменные имена этого уровня должны состоять минимум из трех букв, чтобы не противоречить стандарту ISO 3166, который также определяет правила назначения двухбуквенных кодов стран для доменов второго уровня и ОП.

Примечание О двухбуквенных кодах стран по стандарту ISO 3166 см. также документ \chapt01\articles\iso3166.txt на прилагаемом компакт-диске. Для получения более свежей информации по кодам стран на поисковом узле Интернета введите ключевое слово «ISO3166» или «ISO +3166».

Предполагается, что имя домена первого уровня неизменно. Вот пример правил именования:

Домен	Описание
AFRICA	Африка
CORPIT	Штаб-квартира компании
EUROPE	Австрия, Бельгия, Венгрия, Голландия, Греция, Дания, Ирландия. Испания, Италия, Норвегия, Польша, Португалия, Россия, Румыния, Словакия, Словения, Финляндия, Хорватия, Чешская Республика, Швейцария, Швеция
AT	Совместные предприятия
MEAST	Объединенные Арабские Эмираты, Израиль, Саудовская Аравия, Турция
NOAMER	США и Канада
NOPAC	Гонконг и Web-узлы к северу от него (Япония, Китай, Корея, Тайвань)
PARTNERS	Деловые партнеры и компании-подрядчики
SOAMER	Мексика, Центральная Америка и Южная Америка
SOPAC	Web-узлы южнее Гонконга, включая Индийский полуостров за исключением Афганистана

Внимание! Эти правила именования — лишь пример, согласованный со стандартом ISO 3166. Организация вправе выбрать любые правила именования, соответствующие политике и потребностям.

Домены второго уровня

В идеале должны содержать только коды стран и ответвления от доменов первого уровня. Преимущество этого подхода: ниже доменов второго уровня можно создавать дочерние домены.

Используйте те же правила именования при создании ОП в доменах — это позволит при необходимости повысить ОП до уровня домена с минимальными издержками.

При именовании сайтов в пределах Соединенных Штатов, стандарт ISO 3166 не *применяется*. Вместо этого применяйте двухбуквенные почтовые коды. Единственное исключение — Калифорния, чье двухбуквенное сокращение (CA) аналогично коду Канады по стандарту ISO. Поэтому при создании доменов в Калифорнии используйте сокращение CALIF.

Например, usa.noamer.microsoft.com — домен второго уровня, а ny.usa.noamer.microsoft.com — его дочерний домен.

Планирование организационных подразделений

ОП должны отражать подробности структуры организации. Создание ОП позволяет делегировать полномочия по администрированию небольших групп пользователей, групп и ресурсов. Вы вправе предоставить полный административный контроль (регистрация пользователей, изменение паролей, управление политикой ведения учетных записей и т. п.) или ограниченный (например, только обслуживание очереди печати). Поскольку ОП верхнего уровня способно поддерживать дополнительные уровни ОП, допустимо неограниченно увеличивать степень детализации — объединяйте объекты в логическую структуру, отражающую порядок деятельности Вашего предприятия.

ОП устраняют необходимость предоставлять пользователям административный доступ на уровне домена для выполнения таких задач как, например, создание учетных записей и установка паролей. Теперь можно предоставить пользователям административные полномочия на уровне ОП и тем самым освободить от этого администраторов доменов. ОП добавляет новый уровень защиты путем ограничения видимости общедоступных ресурсов (благодаря ACL) — пользователь видит лишь объекты, к которым имеет доступ. ОП наследует политику безопасности от родительского домена и ОП.

Создание структуры ОП

Целесообразно начинать с разработки структуры ОП для первого домена в пространстве имен. Используйте этот домен и структуру ОП как модель для добавляемых в будущем доменов. Кроме того, созданная структура должна допускать возможные реорганизации с минимальным перемещением объектов.

При создании ОП важно определить, кто сможет просматривать определенные объекты и управлять ими и какими полномочиями в отношении данного объекта будет обладать каждый администратор. Надо также выбрать администраторов, которым будет предоставлен глобальный доступ к некоторым ОП и объектам, и корректно ограничить полномочия остальных администраторов.

Рекомендации по разработке структуры ОП

- Создавайте ОП для делегирования административных полномочий.
- Структура ОП должна быть логичной и осмысленной — это поможет администраторам ОП наиболее эффективно выполнять свои задачи.
- Создавайте ОП для внедрения политики безопасности.
- Создавайте ОП, чтобы ограничить видимость опубликованных ресурсов для определенных пользователей.
- Структуры ОП должны быть относительно статичными. Кроме того, ОП придают гибкость пространству имен, помогая приспособиться к изменяющимся потребностям предприятия.
- Не размещайте в ОП слишком много дочерних объектов.

Приступив к разработке структуры ОП, старайтесь строго придерживаться выбранных правил именования ОП и объектов: имена должны быть иерархичны, статичны и готовы к применению в любом домене предприятия. Не размещайте в ОП слишком много дочерних объектов — это замедлит поиск и выполнение навигационных запросов.

Один из способов создания структуры ОП первого домена — присвоить имя организационным подразделениям верхнего уровня, которые станут заголовками, определяющим более подробные ОП и отнесенные к ним объекты. Альтернативный способ — начать с определения естественной иерархии объектов. Создав иерархические группы объектов, эти

группы можно будет положить в основу организационных подразделений верхнего уровня. Если в сети несколько доменов, структура ОП должна быть применима к каждому из них,

Структура иерархии ОП

Очень важно определить иерархию ОП. Структура доменов многих предприятий отражает характер их деятельности.

Объектно-ориентированная модель деления на ОП

Active Directory разрешает создавать ОП на основе таких объектов, как пользователи, компьютеры, приложения, группы, принтеры, политика безопасности и другие. Правильно разработанная объектно-ориентированная модель ОП заметно облегчает жизнь администраторам подразделений. Обычно это наилучший вариант организации ОП — ведь он обеспечивает минимальное число будущих изменений.

Географическая модель деления на ОП

Можно формировать подразделения, отражающие задачи бизнеса по географическим областям. Скорее всего, такая структура будет стабильна во времени. Впрочем, если Вы предвидите серьезные изменения в организационной структуре предприятия, подумайте о другом принципе разграничения ОП.

Модель деления на ОП по выполняемым задачам

ОП можно создавать на основе различных задач, выполняемых сотрудниками организации, например маркетинг, автоматизация и т. п. Эти задачи, вероятно, останутся даже в случае изменений состава и характеристик выполняющих их отделов.

Модель деления на ОП по отделам

Еше один способ — создать подразделения, отражающие текущую структуру предприятия. Однако структура предприятия нестабильна, так как при реорганизации будет меняться состав отделов или варьироваться возложенные на них задачи.

Модель деления на ОЛ по проектам

Деятельность некоторых предприятий подчинена выполнению конкретных проектов, например в области разработки программ, авиапромышленности и т. п. Можно отразить это и в структуре ОП, однако так делать не рекомендуется, поскольку проекты тоже нестабильны. Обычно такой тип ОП будет дочерним по отношению к другому, более устойчивому ОП. Не забудьте назначить администратора ОП проекта.

Планирование сайта

До этого момента Вы разрабатывали логическую структуру домена и ОП. Успешное внедрение сети Windows 2000 Server на базе Active Directory во многом зависит от физической структуры, которая разграничивается сайтами. *Сайт* (site) — это совокупность одной или нескольких IP-подсетей, соединенных высокоскоростными каналами связи. Зачастую сайт имеет те же границы, что и ЛВС или ГВС сеть, как, например, сети ОС3 SONET (155 Мб/с) или Т3 (45 Мб/с).

Механизм репликации Active Directory позволяет по-разному выполнять репликацию в ЛВС и медленной глобальной сети. Сетевой трафик внутри сайта обычно активнее трафика между сайтами. Настройка сайтов отражается на работе Windows 2000 в двух ключевых моментах.

- **Вход в сеть.** При входе пользователя в сеть Active Directory-совместимые клиенты пытаются найти контроллер домена на сайте компьютера пользователя, чтобы обслужить запрос регистрации в системе и последующие запросы сетевой информации.

- **Репликация каталога.** Расписание и маршрутрепликации каталога домена могут быть сконфигурированы для внутри- и межсайтовой репликации по отдельности. Обычно система настраивается так, чтобы межсайтовая репликация осуществлялась реже, чем внутрисайтовая.

В Active Directory сайты не являются частью пространства имен. Просматривая логическое пространство имен, Вы увидите, что компьютеры и пользователи сгруппированы в домены и ОП, а не в сайты. Структура сайта содержится в отдельной части каталога. Сайты содержат лишь объекты компьютеров и подключений, нужные для конфигурирования межсайтовой репликации.

Правильно спланированные сайты не перегружают сетевые каналы связи трафиком репликации, информация в Active Directory актуальна, и пользователи всегда обращаются к ближайшим ресурсам. „

Группируя подсети в сайты, надо учитывать скорость связи между подсетями.

- Объединяйте только те подсети, которые располагают быстрыми, недорогими и надежными сетевыми соединениями. Под быстрыми здесь понимаются сетевые соединения со свободной пропускной способностью не менее 512 кб/с, которая может быть выделена для трафика репликации. Более емкие соединения разумно рассматривать только для отдельного сайта.
- Конфигурируйте сайтытак, чтобы репликация выполнялась в периоды минимальной нагрузки на сеть.

Структуры домена и сайта хранятся в Active Directory раздельно. Один домен может быть разделен на множество сайтов, а один сайт — включать несколько доменов или их фрагменты (рис. 6-4).

Оптимизация регистрационного трафика

Планируя сайты, определите, какие контроллеры доменов должны использовать для входа в сеть рабочие станции в каждой подсети. Чтобы заставить конкретную рабочую станцию регистрироваться в определенном наборе контроллеров доменов, в рамках сайта рабочей станции должны находится только необходимые контроллеры.

Оптимизация репликации каталога

Планируя сайты, решите, где разместить контроллеры доменов. Поскольку любой контроллер домена должен участвовать в репликации каталога совместно с другими контроллерами своего домена, сайты надо сконфигурировать так, чтобы репликация не мешала работе сети.

Вот как распределять сайты в зависимости от размеров филиалов:

Количество рабочих станций	Создавать сайт?	Примечания
1-5	Нет	Аутентификация пользователей осуществляется по низкоскоростным каналам связи, которые не годятся для трафика доменной репликации.
Более 5	Да	Для ускорения аутентификации пользователей в локальном сайте размещайте контроллеры доменов локально. Трафик репликации на низкоскоростных каналах надо настроить так, чтобы репликация осуществлялась в периоды минимальной нагрузки и с более длительными интервалами.

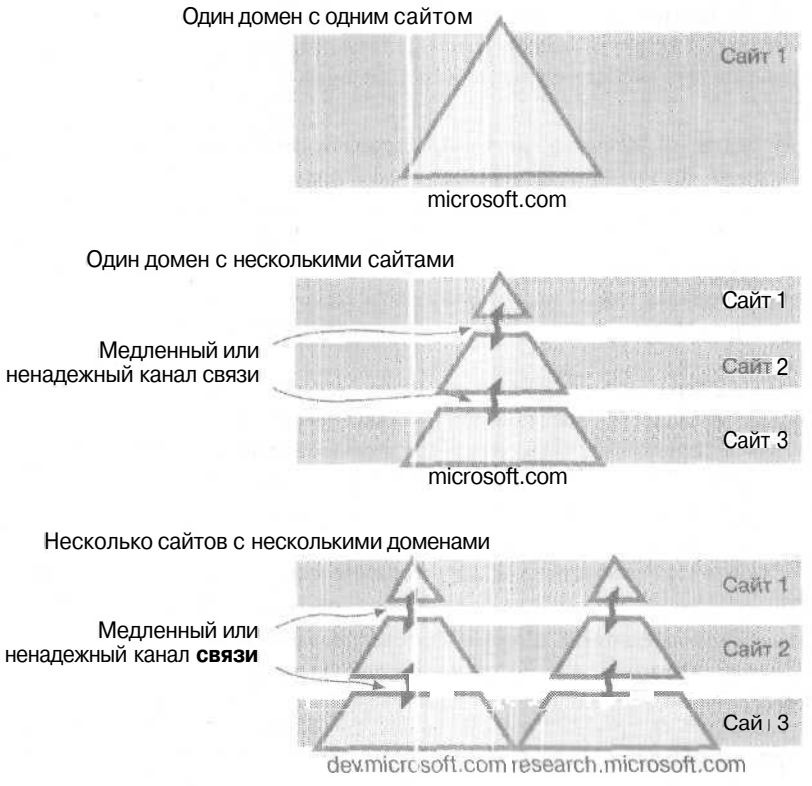


Рис. *6-4.* Один домен *с* одним сайтом, один домен с несколькими сайтами и несколько сайтов с несколькими доменами

Резюме

При подготовке к внедрению Active **Directory надо** тщательно спланировать **структуру пространства имен, ОП и сайтов. Вам** надо **определить,** будут **ли внутреннее и внешнее пространства имен одинаковыми** или раздельными. **В первом случае доменное имя верхнего уровня** будет **одинаковым с** разных сторон **брандмауэра, во втором — будет различаться. Кроме пространства имен,** надо **спланировать деление на ОП; оно должно отражать структуру предприятия,** а также способы **работы и организации деятельности** сотрудников. Сайты **надо** тщательно спланировать **еше до** внедрения Active **Directory. Объединяйте** лишь подсети, **располагающие емкими, недорогими и надежными каналами связи. Сайты** должны **быть** сконфигурированы так, чтобы **трафик** репликации **не снижал производительность** сети.

Занятие 3. Внедрение Active Directory

Здесь мы обсудим установку Active Directory на компьютер Windows 2000 Server, включая описание работы с соответствующим мастером. Мы также рассмотрим базу данных и общий системный том, создаваемые в ходе установки Active Directory. В конце занятия описываются файл Ntds.dit и режимы домена.

Изучив материал этого занятия, Вы сможете:

- ✓ установить Active Directory на компьютер Windows 2000 Server.

Продолжительность занятия — около 30 минут.

Мастер установки Active Directory

Мастер Active Directory Installation (Мастер установки Active Directory) позволяет:

- добавить контроллер домена к существующему домену;
- создать первый контроллер нового домена;
- создать новый дочерний домен;
- создать новое дерево доменов.

Для запуска мастера Active Directory Installation раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Configure Your Server (Настройка сервера). На левой панели открывшегося окна щелкните ссылку Active Directory, прокрутите содержимое окна вниз и выберите ссылку вызова мастера. Или запустите утилиту dcpromo.exe из окна Run или из командной строки. В любом случае откроется окно мастера, который поможет Вам установить Active Directory на компьютер и создать контроллер домена.

При установке Active Directory Вы сможете выбрать: добавить ли новый контроллер к существующему домену, или создать первый контроллер для нового домена (рис. 6-5).

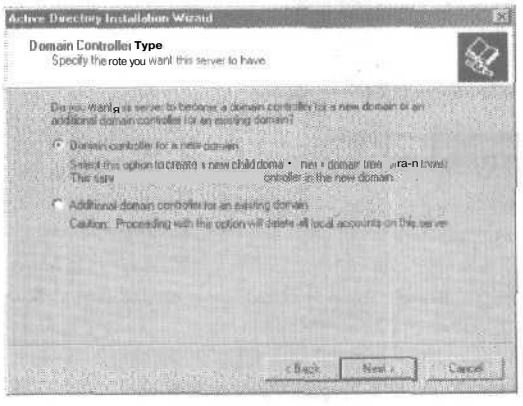


Рис. 6-5. Окно Domain Controller Type (Тип контроллера домена)

Добавление контроллера домена к существующему домену

Если Вы решили добавить контроллер домена к существующему домену, будет создан дополнительный контроллер домена. Такие контроллеры создаются для избыточности и уменьшения нагрузки на существующие контроллеры доменов.

Создание **первого контроллера нового** домена

При создании первого контроллера нового домена Вам придется создавать и новый домен, Домены создаются для распределения информации, что позволяет масштабировать Active Directory для удовлетворения потребностей очень больших организаций.

Вы вправе создать дочерний домен или новое дерево доменов. В первом случае новый домен добавляется в качестве дочернего к существующему домену. Во втором случае новый домен не будет являться частью существующего ломена, и Вы сможете создать новый лес доменов или присоединиться к существующему лесу.

Внимание! Запуск утилиты dcpromo.exe на контроллере домена позволит Вам удалить службы Active Directory с контроллера домена и превратить его в изолированный сервер. Удаление Active Directory со всех контроллеров данного домена приведет к удалению БД каталога домена, после чего домен прекратит существование.

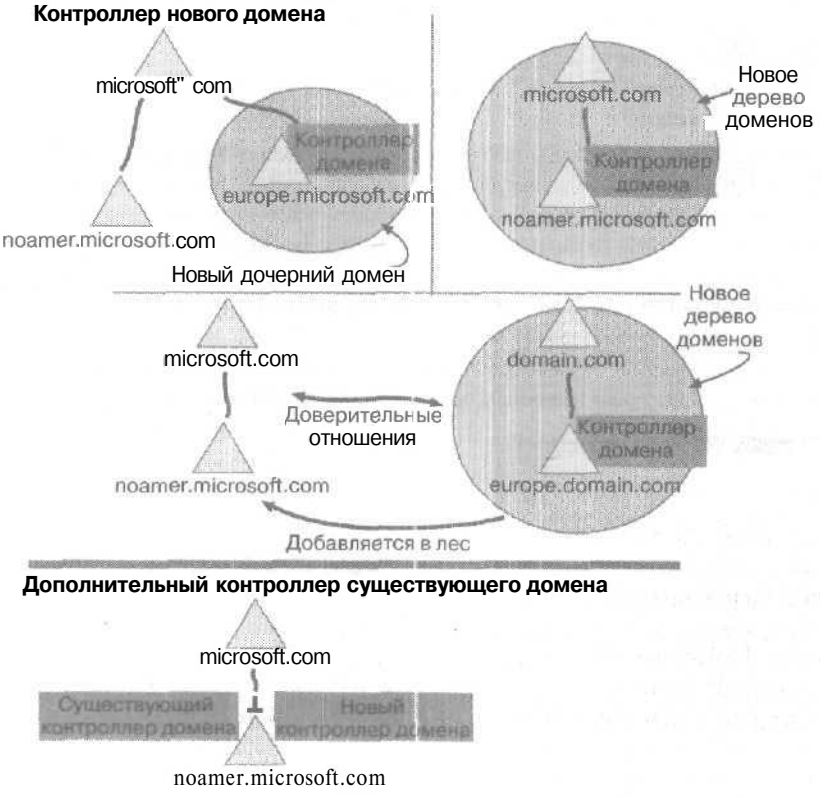


Рис. 6-6. Графическое представление различных типов контроллеров доменов

База данных и общий системный том

При установке Active Directory автоматически создаются БД, файлы ее журнала и общий системный том.

База данных Active Directory

Это каталог нового домена. По умолчанию БД и файлы ее журнала размешаются в папке %systemroot%\Ntds. Впрочем, в ходе установки Active Directory допустимо указать другой каталог. Для повышения производительности разместите БД и файлы ее журнала на отдельном жестком диске. Лучше всего разместить БД на аппаратной RAID-системе, например RAID-5 или RAID-10 (зеркальное отображение с чередованием дисков) — это обеспечит отказоустойчивость и высокую производительность.

БД каталога фактически хранится в файле Ntds.dit, где находится вся информация хранилища Active Directory. Это БД ESE, содержащая полную схему, глобальный каталог и все объекты, хранимые на контроллере домена. В процессе повышения статуса до уровня контроллера Ntds.dit переносится из каталога %systemroot%\System32 в указанный каталог. Затем службы Active Directory стартуют с новой копии этого файла, а если есть и другие контроллеры домена, то в процессе репликации обновляют этот файл данными от других контроллеров.

Общий системный том

Существует на всех контроллерах домена Windows 2000, хранит сценарии и некоторые объекты групповой политики для текущего домена и предприятия в целом. По умолчанию общий системный том размещается в папке %systemroot%\Sysvol, причем он может храниться только на диске или разделе с файловой системой NTFS 5.0.

Репликация общего системного тома идет по тому же расписанию, что и репликация Active Directory, поэтому Вы можете не заметить репликацию файла в/из нового системного тома, пока не пройдет два цикла репликации (обычно это требует минут 10). Дело в том, что первый цикл репликации файла обновляет конфигурацию других системных томов, уведомляя их о добавлении нового системного тома.

Режимыдомена

Существуют два режима домена: смешанный (Mixed) и основной (Native).

Смешанный режим

При первой установке или обновлении контроллера домена до Windows 2000 Server контроллер запускается в смешанном режиме, позволяющем ему взаимодействовать с любыми контроллерами доменов под управлением Windows NT 3.51 или 4.0. Кроме того, смешанный режим нужен для входа в сеть любому клиенту, использующему аутентификацию NTLM и службу каталога Windows NT 3.51 или Windows NT 4.0. Им также требуется WINS для разрешения имен. Эти клиенты нижнего уровня обычно будут аутентифицироваться в Windows 2000 Server прежде, чем Windows NT Server нижнего уровня удовлетворит их запрос на вход в систему. Компьютер с Windows 2000 Server также всегда становится *координатором сети* (master browser). Выполнение этих функций создает дополнительную нагрузку на контроллеры доменов Windows 2000 Server.

Основной режим

Если на всех контроллерах домена установлен Windows 2000 Server и Вы не собираетесь больше добавлять в этот домен контроллеры нижнего уровня, переведите домен в основной режим.

При изменении режима со смешанного на основной происходит следующее:

- прекращается поддержка репликации нижнего уровня, после чего в этом домене больше нельзя будет иметь контроллеры, управляемые предыдущими версиями Windows;
- запрещается **добавление новых** контроллеров **нижнего уровня в данный** домен;
- сервер, исполнявший роль ОСНОЕНОГО контроллера домена, перестает быть основным; все контроллеры становятся равноправными.

Примечание Изменения режима домена носят однонаправленный характер. Вы не сможете перейти из основного режима в смешанный.

Упражнение 1: **установка** Active Directory

Сделайте изолированный сервер Server01 первым контроллером домена в дереве Active Directory. В ходе установки будет настроена и сконфигурирована служба DNS для разрешения имен В следующей главе Вы подробнее изучите DNS и DHCP. Выполняйте упражнение на Server01.

▶ Задание 1: повысьте изолированный сервер до контроллера домена

С помощью программы dcpromo.exe установите Active Directory и службу DNS на изолированный сервер (ServerOl) и превратите его в контроллер и DNS-сервер нового домена.

1. Зарегистрируйтесь на ServerOl как Administrator (Администратор) с паролем **password.**
2. Если откроется окно Windows 2000 Configure Server (Настройка сервера Windows 2000), закройте его, так как для выполнения этого упражнения Вы используете утилиту dcpromo.exe.
3. Вставьте установочный компакт-диск Windows 2000 Server в привод CD-ROM на Server01.

   Компакт-диск необходим для установки службы DNS в ходе работы dcpromo.exe.
4. Если сработает программа автозапуска, закройте ее окно, щелкнув ссылку Exit (Выход).
5. В меню Start (Пуск) выберите команду Run (Выполнить).
6. В диалоговом окне Run (Запуск программы) наберите **dcpromo.exe** и щелкните кнопку OK.

   Откроется окно мастера Active Directory Installation (Мастер установки Active Directory).
7. Щелкните кнопку Next (Далее).

   Откроется окно Domain Controller Type (Тип контроллера домена).
8. Выберите Domain Controller For Л New Domain (Контроллер домена в новом домене) и щелкните кнопку Next (Далее).

   Откроется окно Create Tree Or Child Domain (Создание дерева или дочернего домена).
9. Убедитесь, что выбран переключатель Create A New Domain Tree (Создать новое доменное дерево) и щелкните кнопку Next (Далее).

   Откроется окно Create Or Join Forest (Создание леса или присоединение к лесу).
10. Щелкните переключатель Create A New Forest Of Domain Trees (Создать новый лес доменных деревьев) и щелкните Next (Далее).

    Откроется окно New Domain Name (Имя DNS-домена).
11. В поле Full DNS Name For The New Domain введите **microsoft.com** и щелкните кнопку Next (Далее).

    Откроется окно NetBIOS Domain Name (NetBIOS-имя домена).
12. Убедитесь, что в поле Domain NetBIOS Name (NetBIOS-имя домена) выведено MICROSOFT и щелкните кнопку Next (Далее).

    Откроется окно Database And Log Locations (Местоположение базы данных и журнала).

13. Убедитесь, что для размещения базы данных и протокола выбран путь C:\Winnt\ Ntds и щелкните кнопку Next (Далее).
    Откроется окно Shared System Volume (Общий доступ к системному тому).
14. Изучите информацию в этом окне и убедитесь, что для размещения SYSVOL указан путь C:\WINNT\SYSVOL.
15. Щелкните кнопку Next (Далее).
    Появится сообщение, что мастер не может связаться с DNS-сервером, обрабатывающим имя microsoft.com.
16. Щелкните кнопку OK.
    Поскольку мастер не нашел DNS-сервер, откроется окно Configure DNS (Настройка DNS).
17. Убедитесь, что выбран переключатель Yes, Install And Configure DNS On The Computer (Recommended) (Да, автоматически установить и настроить DNS) и щелкните кнопку Next (Далее).
    Откроется окно Permissions (Разрешения).
18. Первоначально контроллер домена запустится в смешанном режиме, поэтому убедитесь, что выбран переключатель Permissions Compatible With Pre-Windows 2000 Servers (Разрешения, совместимые с серверами пред-Windows 2000) и щелкните кнопку Next (Далее).
    Откроется окно Directory Services Restore Mode Administrator Password (Пароль администратора для режима восстановления).
19. Изучите информацию в этом окне, а затем наберите password в обоих полях и щелкните кнопку Next (Далее).
    Откроется окно Summary (Сводка), представляющее список выбранных Вами параметров установки.
20. Изучите содержание этого окна и щелкните кнопку Next (Далее).
    Появится индикатор хода установки Configuring Active Directory (Идет настройка Active Directory).
    Этот процесс займет несколько минут. Проверьте, вставлен ли установочный компакт-диск Windows 2000 Server в Server01 — он понадобится для установки службы DN S.
21. Когда откроется окно Completing The Active Directory Installation Wizard (Завершение работы мастера установки Active Directory), выньте компакт-диск из привода, щелкните кнопку Finish (Готово) и перезагрузите компьютер.
    Первый запуск Windows 2000 Server в роли контроллера домена проходит медленнее обычного.

▶ Задание 2: просмотрите Ваш домен

1. Зарегистрируйтесь на Вашем сервере как Administrator (Администратор) с паролем password.
2. Дважды щелкните значок My Network Places (Мое сетевое окружение).
   Откроется одноименное окно.
3. Дважды щелкните значок Entire Network (Вся сеть), а затем — ссылку на левой стороне окна You May Also View The Entire Contents Of The Network (Можно также просмотреть все содержимое сети).
4. Дважды щелкните значок Microsoft Windows Network (Сеть Microsoft Windows).
5. Закройте окно My Network Places (Мое сетевое окружение).

▶ Задание 3: задействуйте Active Directory Manager

Просмотрите домен с помощью оснастки Active Directory Users And Computers.

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Active Directory Users And Computers (Active Directory – пользователи и компьютеры).

   Откроется окно оснастки Active Directory Users And Computers (Active Directory – пользователи и компьютеры).
2. В дереве консоли щелкните знак «+» слева от microsoft.com.
3. Проверьте каждый из контейнеров, входящих в microsoft.com. Не меняйте информацию в этих контейнерах.

   Что представляют собой пункты ниже microsoft.com и каково их назначение? Подсказка: изучите свойства каждого контейнера в дереве консоли, чтобы узнать об их назначении.
4. Закройте оснастку Active Directory Users And Computers.

Упражнение 2: присоединение Server02 к домену

Присоедините Server02 к домену microsoft.com. Поскольку DHCP пока не используется, вручную сконфигурируйте IP-адреса Server01 и Server02. После присоединения Server02 к домену для него будет создана учетная запись компьютера, которая появится в хранилище Active Directory. В упражнении используются оба компьютера.

▶ Задание 1: вручную настройте IP-адреса и присоедините Server02 к домену microsoft.com

1. Зарегистрируйтесь на ServerOl и Server02 как Administrator (Администратор) с паролем **password.**
2. На ServerOl раскройте меню Start\Settings (Пуск\Настройка) и щелкните ярлык Network And Dial-Up Connections (Сеть и удаленный доступ к сети).

   Откроется одноименное окно.
3. Щелкните значок Local Area Connection (Подключение по локальной сети) и в меню File (Файл) выберите команду Properties (Свойства).

   Откроется диалоговое окно свойств локального соединения.
4. Перейдите на вкладку Network (Сеть) и в списке Components Checked Are Used By This Connection (Отмеченные компоненты используются этим подключением) выберите Internet Protocol **(TCP/IP).**
5. Щелкните кнопку Properties (Свойства).

   Откроется диалоговое окно свойств TCP/IP.
6. Щелкните переключатель Use The Following IP Address (Использовать следующий IP-адрес).
7. В поле IP Address (IP-адрес) введите **10.10.10.1.**
8. Убедитесь, что в поле Subnet Mask (Маска подсети) появилось значение 255.0.0.0.
9. Щелкните переключатель Use The Following DNS Server Addresses (Использовать следующие адреса DNS-серверов).
10. В поле Preferred DNS Server (Предпочитаемый DNS-сервер) введите **10.10.10.1.**
11. Два раза щелкните кнопку OK, чтобы закрыть окна свойств.
12. Перейдите к Server02 и повторите пп. 2–9 настоящей инструкции.
13. В поле IP Address введите **10.10.10.2.**
14. Проверьте, что в поле Subnet Mask появилось значение 255.0.0.0.

15. Щелкните переключатель Use The Following DNS Server Addresses.
16. В поле Preferred DNS Server наберите **10.10.10.1.**
17. Два раза щелкните кнопку OK, чтобы закрыть окна свойств.
18. На Server02 откройте Control Panel (Панель управления).
19. Дважды щелкните значок System (Система).
20. В открывшемся окне щелкните вкладку Network Identification (Сетевая идентификация), а затем — кнопку Properties (Свойства),

    Откроется диалоговое окно Identification Changes (Изменение идентификации).
21. Щелкните переключатель Domain (Домен), наберите microsoft и щелкните кнопку OK.
22. В открывшемся окне в поле Name введите **administrator,** а в поле Password — **password.** Затем щелкните кнопку OK.
23. Через некоторое время появится сообщение Network Identification (Сетевая идентификация), приветствующее Вас при входе в домен.
24. Щелкните кнопку OK.

    Появится сообщение, что для вступления изменений в силу надо перезагрузить компьютер.
25. Щелкните кнопку OK.

    Вы вернетесь в окно System Properties (Свойства системы).
26. Щелкните кнопку OK.

    В диалоговом окне System Settings Change (Изменение параметров системы) Вам будет предложено перезагрузить компьютер, чтобы изменения вступили в силу,
27. Щелкните кнопку Yes, чтобы перезагрузить Server02.
28. С Server02 войдите в домен microsoft.com как Administrator (Администратор) с паролем password.
29. Если откроется окно Configure Your Server (Настройка сервера Windows 2000), сбросьте флажок Show This Screen At Startup (Показывать это окно при загрузке) и закройте окно.

Упражнение 3: установка дополнительных средств администрирования из пакета Adminpak.msi

Изучите инструменты из группы Administrative Tools (Администрирование), а затем установите дополнительные средства из пакета Adminpak.msi. Упражнение выполняйте на Server01.

▶ Задание 1: измените меню Start (Пуск) и изучите новые средства администрирования

1. Зарегистрируйтесь на ServerOl как администратор с паролем **password.**
2. Раскройте меню Start\Settings (Пуск\Настройки) и щелкните ярлык Taskbar And Start menu (Панель задач и меню «Пуск»).

   Откроется диалоговое окно Taskbar And Start Menu Properties (Свойства: Панель задач и меню «Пуск»).
3. Сбросьте флажок Use Personalized Menus (Использовать сокращенные меню) и щелкните кнопку OK.
4. Раскройте меню Start\Programs (Пуск\Программы) и щелкните ярлык Administrative Tools (Администрирование).

   Заметьте: теперь в меню Administrative Tools перечислены все установленные программы, а не только наиболее часто используемые.

Когда Server01 был отдельным сервером, в меню Administrative Tools отображались все приложения, кроме специфичных для Active Directory, домена и сопровождения DNS. Наведите указатель мыши на ярлыки следующих приложений и изучите текст всплывающих подсказок:

- Active Directory Domains and Trusts (Active Directory — домены и доверие);
- Active Directory Sites and Services (Active Directory — сайты и службы);
- Active Directory Users and Computers (Active Directory — пользователи и компьютеры);
- DNS.

▶ **Задание 2: установите дополнительные** средства **администрирования**

Установите пакет Windows 2000 Administrative Pack на ServerOl. Инструменты из его состава также можно установить на Windows 2000 Professional, чтобы выполнять дистанционное администрирование серверов Windows 2000.

1. В меню Start (Пуск) выберите команду Run (Выполнить).
   Откроется диалоговое окно Run (Запуск программы).
2. Наберите **adminpak.msi.**
   Файл adminpak.msi находится в каталоге C:\WINNT\system32, который указан в переменной среды PATH, поэтому вводить путь к этому файлу не надо.
3. Щелкните кнопку OK.
   Откроется окно мастера Windows 2000 Administration Tools Setup Wizard (Мастер установки Администрирование Windows 2000)
4. Изучите информацию в его первом окне и щелкните кнопку Next (Далее).
   Откроется окно Setup Options (Параметры установки).
5. Щелкните переключатель Install All Of The Administrative Tools (Установка всех средств администрирования), а затем — Next (Далее).
   При установке средств администрирования откроется окно Installation Progress (Индикатор установки).
6. Когда откроется окно Completing The Windows 2000 Administration Tools Setup Wizard (Завершение работы мастера установки Администрирование Windows 2000), щелкните кнопку Finish (Готово), чтобы завершить установку.
7. Раскрыв меню Administrative Tools (Администрирование), просмотрите ярлыки установленных средств. Для определения назначения служебной программы наведите на ее ярлык указатель мыши и прочтите всплывающую подсказку.

Упражнение 4: преобразование изолированного корня DFS в доменный

В главе 5 Вы создали изолированный корень DFS. Удалите его и создайте доменный корень DFS и его реплику. Это стало возможно, поскольку теперь Вы используете контроллер домена.

▶ **Задание 1: удалите изолированный корень DFS**

На сервере может существовать только один корень DFS. Следовательно, надо вначале удалить изолированный корень DFS на Server01.

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Distributed File System (Распределенная файловая система **DFS).**
   Откроется окно оснастки Distributed File System.

2. В дереве консоли щелкните ссылку \\SERVER01\Public.
3. В меню Action (Действие) выберите команду Delete DFS Root (Удалить корень DFS).

   Появится сообщение, что клиенты больше не смогут получить доступ к этому корню DFS. Общие ресурсы, связанные с корнем DFS, при этом не удаляются.
4. Щелкните кнопку Yes (Да).

► Задание 2: создайте доменный корень DFS

Доменный корень конфигурируется аналогично изолированному, он обеспечивает репликацию. Выполняйте это упражнение на Server01.

1. В дереве консоли оснастки Distributed File System (Распределенная файловая система DFS) щелкните Distributed File System (Распределенная файловая система DFS).
2. В меню Action (Действие) выберите команду New DFS Root (Создать корень DFS).
3. Щелкните кнопку Next (Далее).

   Откроется окно Select The DFS Root Type (Выбор типа корня DFS).
4. Отметьте переключатель Create A Domain DFS Root (Создать корень DFS в домене) и щелкните кнопку Next (Далее).

   Откроется окно Select The Host Domain For The DFS Root (Укажите несущий домен для корня DFS), в полях Domain Name (имя домена) и Trusting Domains (Домены-доверители) которого значится *microsoft.com*.
5. Щелкните кнопку Next (Далее).

   Откроется окно Specify The Host Server For The DFS Root (Выбор несущего сервера для корня DFS). В поле Server Name (Имя сервера) значится server01.microsoft.com. Если бы ServerOl все еще обслуживал изолированный корень DFS, этого бы не произошло. Это сделано намеренно, так как сервер может обслуживать только один корень DFS.
6. Щелкните кнопку Next (Далее).

   Откроется окно Specify The DFS Root Share (Выбор общего ресурса для корня DFS).
7. Убедитесь, что выбран переключатель Use An Existing Share (Использовать существующий общий ресурс), и выберите из раскрывающегося списка пункт Public.
8. Щелкните кнопку Next (Далее).
9. В окне Name The DFS Root (Выбор имени для корня DFS) в поле Comment (Комментарий) введите **Public** access **share** и щелкните кнопку Next (Далее).
10. Проверьте перечисленные в окне Completing The New DFS Root Wizard (Завершение работы мастера создания нового корня DFS) параметры нового корня. Заметьте: несущим сервером является SERVER01.microsoft.com. При создании изолированного корня DFS это был бы SERVER01.
11. Щелкните кнопку Finish (Готово).

    Вы вернетесь в окно оснастки Distributed File System, где новый корень DFS будет отображаться как \\microsoft.com\Public.

► Задание 3: создайте реплику корня DFS

Создайте реплику корня \\SERVER01\Public на Server02, ставшего в упражнении 2 частью домена microsoft.com.

1. На ServerOl в оснастке Distributed File System выберите в дереве консоли \\microsoft.com\Public.

   На правой панели появится корень DFS — \\SERVER01\Public.
2. В меню Action (Действие) выберите команду New Root Replica (Создать корневую реплику).

Откроется окно Specify The Host Server For The DFS Root (Выбор несущего сервера для корня DFS).

3. В поле Server Name (Имя сервера) введите Server02 и щелкните кнопку Next (Далее).
   Доменный корень DFS можно реплицировать на другой сервер в домене (контроллер или рядовой сервер),
   Откроется окно Specify The DFS Root Share (Выбор общего ресурса для корня DFS).
4. Щелкните переключатель Use An Existing Share (Использовать существующий общий ресурс).
5. В раскрывающемся списке выберите pubrepl.
6. Щелкните кнопку Finish (Готово).
   Появится сообщение, что папка \\Server02\c$\publicrepl не существует.
7. Щелкните кнопку Yes (Да) для создания панки.

► Задание 4: включите службу FRS для создания реплики корня DFS

Настройте политику репликации, чтобы корень DFS автоматически синхронизировался со своей репликой.

1. На компьютере Server01 выберите в дереве консоли оснастки Distributed File System ссылку \\microsoft.com\Public.
   На правой панели появятся корень DFS \\SERVER01\Public и \\SERVER02\pubrepl.
2. В меню Action (Действие) выберите команду Replication Policy (Политика репликации).
3. Щелкните \\SERVER01\Public, а затем — кнопку Set Master (Основной).
4. Щелкните \\SERVER02\pubrepl, а затем — кнопку Enable (Включить) для включения репликации.
5. Щелкните кнопку OK, чтобы закрыть диалоговое окно Replication Policy (Политика репликации).

► Задание 5: создайте DFS-ссылки

Воссоздайте DFS-ссылки, которые Вы уже создавали в упражнении 1 главы 5.

1. На ServerOl в дереве консоли оснастки Distributed File System выберите \\microsoft.com\Public.
2. В меню Action (Действие) выберите команду New DFS Link (Создать ссылку DFS).
   Откроется диалоговое окно Create A New DFS Link (Создание новой ссылки DFS).
3. В поле Link Name (Имя ссылки) введите intranet.
4. В поле Send The User To This Shared Folder (Переадресовать пользователя на эту общую папку) введите \\Server02\internal.
5. В поле Comment (Комментарий) введите **Internal web content** и щелкните кнопку OK.
6. Повторите п. 3–5 для создания новых ссылок DFS согласно информации из таблицы.

Наименование ссылки	Отсылать пользователя к этому общему каталогу	Комментарий
news	\\Server01\Press	Текущие пресс-релизы
ftp	\\Server01\ftproot	Корневой каталог FTP-узла
tech	\\Server01\TechDocs	Техническая документация

7. На компьютере Server02 откройте C:\Publicrepl (реплика корня DFS). Вы увидите реплики новых папок, появившиеся в корне DFS.

Резюме

Для установки Active Directory на компьютер Windows 2000 Server применяется мастер Active Directory Installation (Мастер установки Active Directory). Этот мастер также позволяет добавить контроллер в существующий домен, создать первый контроллер домена, дочерний домен и новое дерево доменов. При установке Active Directory автоматически создаются база данных, файлы ее журнала и общий системный том. БД каталога находится в файле Ntds.dit, который является хранилищем Active Directory- Общий системный том — это структура каталога, существующая на всех контроллерах домена Windows 2000. Он хранит сценарии и некоторые объекты групповой политики для текущего домена и для предприятия в целом. Домен может работать в смешанном или основном режиме. При первоначальной установке или обновлении контроллера домена до Windows 2000 Server контроллеры запускаются в смешанном режиме. Если все контроллеры домена переведены на Windows 2000 Server и Вы больше не собираетесь добавлять к домену контроллеры на базе предыдущих версий Windows, переведите домен в основной режим.

Занятие 4. Администрирование Active Directory

После установки Active Directory можно приступить к созданию объектов и управлению ими. Здесь обсуждается создание ОП и добавление в них объектов, подробно описано управление созданными объектами: как их найти, изменить или уничтожить. И в заключение мы рассмотрим управление доступом к объектам, включая разрешения Active Directory и полномочия административного управления объектами.

Изучив материал этого занятия, Вы сможете:

- ✓ создавать ОП и объекты в них;
- ✓ находить, изменять, перемешать и удалять созданные Вами объекты;
- ✓ ограничивать доступ к объектам Active Directory.

Продолжительность занятия — около 50 минут.

Создание подразделений и объектов в них

Объект Active Directory — это уникальный именованный набор атрибутов, представляющий определенный сетевой ресурс. Л ри добавлении в сеть новых ресурсов, таких как учетная запись пользователя, группа или принтер, Вы создаете новый объект Active Directory, представляющий этот ресурс. Перед добавлением объектов в Active Directory надо создать ОП, которое будет содержать эти объекты.

Создание ОП

Вы можете создать ОП в рамках домена, объекта Domain Controller или другого ОП. В созданное ОП можно добавлять объекты.

Для создания ОП Вы должны обладать полномочиями по добавлению подразделений в родительское ОП, домен или узел Domain Controller, где Вы хотите создать ОП. По умолчанию такими полномочиями наделена группа Administrators (Администраторы). Вы не сможете создавать ОП в большинстве стандартных контейнеров, таких как Computers или Users.

ОП создаются для упрощения администрирования сети. Структура ОП должна основываться на конкретных задачах администрирования. Вы можете легко изменять структуру ОП или перемешать объекты между ОП.

Вы должны создавать ОП в следующих случаях:

- чтобы предоставить административные полномочия другим пользователям или администраторам;
- для группирования объектов, над которыми выполняются сходные административные операции; это облегчает поиск сходных сетевых ресурсов и их обслуживание — так, можно объединить в одном ОП все объекты User для временных служащих;
- для ограничения видимости сетевых ресурсов вхранилище Active Directory — пользователи увидят только те объекты, к которым имеют доступ; разрешения для ОП можно легко изменить, ограничив доступ к конфиденциальной информации.

Вы можете создать ОП с помощью оснастки Active Directory Users and Computers (Active Directory — пользователи и компьютеры), выделив домен или существующее ОП для размещения нового ОП. В меню Action (Действие) выберите New (Создать), а затем — команду Organizational Unit (Подразделение) (рис. 6-7). Введите имя нового ОП в поле Name (Имя) и щелкните кнопку OK.

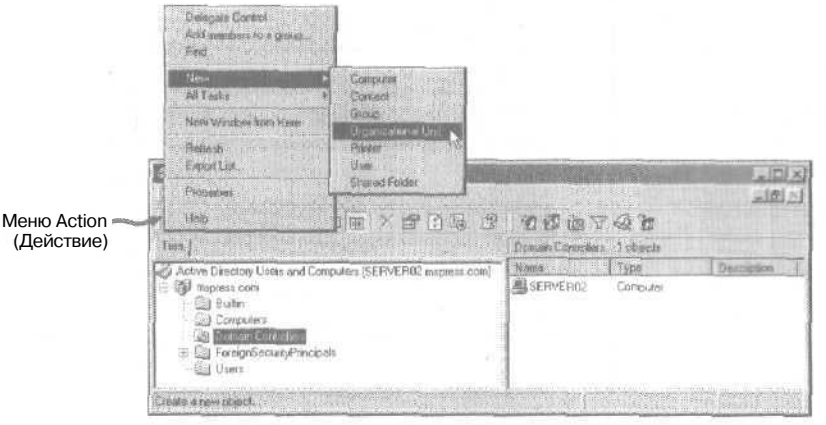


Рис. 6-7. **Создание ОП в оснастке Active Directory Users and Computers** (Active **Directory — пользователи и компьютеры)**

Добавление объектов в ОП

Для добавления объектов в ОП Вы должны обладать в нем соответствующими полномочиями. По умолчанию такие права предоставлены группе Administrators. Разновидности создаваемых объектов зависят от правил схемы, используемого мастера или оснастки. Некоторые атрибуты объекта можно определить только после его создания.

Экземпляры объекта создаются в оснастке Active Directory Users and Computers, Выделите ОП, в которое надо добавить объект, в меню Action (Действие) выберите New (Создать) и щелкните нужный тип объекта. В открывшемся диалоговом окне введите значения атрибутов объекта.

Примечание Атрибуты объекта в схеме (или свойства) — это категории информации, определяющие характеристики всех экземпляров определенного типа объекта. У всех экземпляров объекта набор атрибутов одинаков — уникальным объект делают значения атрибутов. Например, все экземпляры объекта User имеют атрибут First Name, однако значение этого атрибута может быть любым именем, например Linda иди Max.

Описание объектов Active Directory

Добавление в сеть новых ресурсов приводит к созданию новых объектов Active Directory, представляющих эти ресурсы. Вот наиболее общие типы объектов, которые можно добавлять в Active Directory.

Значок	Объект	Описание
	Computer (Компьютер)	Представляет компьютер в сети. Для компьютеров Windows NT Workstation и Windows NT Server это будет учетная запись компьютера. Объект содержит сведения о компьютере, входящем в домен.
	Contact (Контакт)	Учетная запись без ограничений по доступу. Вы не сможете войти в сеть как Contact. Объекты Contact обычно применяются для представления внешних пользователей в электронной почте.

(окончание)

Значок	Объект	Описание
	Group (Группа)	Включает пользователей, компьютеры и другие группы, упрощает обслуживание большого числа объектов.
	Printer (Принтер)	Сетевой принтер, опубликованный в каталоге. В действительности это ссылка на подключенный к компьютеру принтер. Вы можете вручную опубликовать принтер в Active Directory
	User (Пользователь)	Главный элемент системы безопасности в каталоге. Данные, содержащиеся в этом объекте, позволяют пользователю входить в систему Windows 2000. Содержит множество дополнительных полей, таких как имя, фамилия, псевдоним и адрес электронной почты.
	Shared Folder (Общая папка)	Общий ресурс, опубликованный в каталоге. На самом деле **это ссылка на общую** папку — **содержит** адрес **данных, а не сами данные.**

Упражнение 5: создание ОП и их объектов

Создайте ОП и три учетные записи пользователей, которые будут применяться в дальнейшем.

► **Задание 1: создайте экземпляры ОП и объектов User**

Создайте два ОП и три объекта User.

1. Зарегистрируйтесь на Server01 как Administrator (Администратор) с паролем **password.**
2. Откройте оснастку Active Directory Users And Computers (Active Directory — пользователи и компьютеры).

   Для уверенности в правильном размещения нового ОП сначала выберите место размещения.
3. В дереве консоли щелкните microsoft.com.
4. В меню Action (Действие) выберите New (Создать), а затем —команду Organizational Unit (Подразделение).

   Откроется диалоговое окно New Object — Organizational Unit (Новый объект — Подразделение).

   Заметьте: в имени заключена только требуемая информация. В диалоговом окне будет представлено местоположение, где будет создан объект. Это должно быть microsoft.com/.
5. В поле Name (Имя) введите **Sales** и щелкните кнопку OK.

   В дереве консоли появится ОП с именем Sales.
6. В microsoft.com создайте также еше одно ОП *с* именем Servers.
7. В дереве консоли щелкните Users.
8. В меню Action (Действие) выберите New (Создать), а затем — команду User (Пользователь).

   Диалоговое окно New Object — User (Новый объект — Пользователь) сообщает, что новая учетная запись пользователя будет создана в ОП microsoft.com/Users.

Примечание Объекты User разрешается создавать в любом ОП, хотя далее Вы будете создавать большинство таких объектов в ОП Users.

9. Создайте новую учетную запись пользователя с параметрами:

Поле	Значение
First name (Имя)	Jane
Last name (Фамилия)	Doe
User logon name (Имя входа пользователя)	Jane_Doe

10. Щелкните кнопку Next (Далее).
11. Оставьте поля пароля незаполненными и не изменяйте стандартные параметры этой учетной записи. Щелкните кнопку Next (Далее).

    Откроется итоговое окно, представляющее полное и регистрационное имя для пользователя Jane Doe.
12. Щелкните кнопку Finish (Готово).
13. На правой панели оснастки Active Directory Users And Computers щелкните объект Jane_Doe.
14. В меню Action (Действие) выберите команду Properties (Свойства).

    Откроется диалоговое окно свойств этого объекта.
15. На вкладке General (Общие) диалогового окна свойств в поле Telephone Number (Номер телефона) наберите 555-1234.
16. Щелкните кнопку OK.
17. Создайте учетные записи пользователей с параметрами:

Поле	Значение
First name (Имя)	John
Last name (Фамилия)	Smith
User logon name (Имя входа пользователя)	John_Smith

Поле	Значение
First **name (Имя)**	**Bob**
Last name (Фамилия)	Train
User **logon** name **(Имя** входа пользователя)	Bob_Train

Вы используете эти учетные записи в следующей главе.

Управление объектами Active Directory

Включает поиск объектов, их изменение, уничтожение или перемещение. В двух последних случаях надо иметь соответствующие разрешения для объекта или для ОП, куда Вы перемешаете объект. По умолчанию данными полномочиями обладают все члены группы Administrators.

Поиск объектов

Глобальный каталог (ГК) содержит частичную реплику всего каталога и хранит информацию обо всех объектах в дереве доменов или лесе. Поэтому пользователь может найти

объект независимо от его расположения в домене или лесе. Содержание ГК автоматически генерируется по сведениям из доменов, составляющих каталог.

Для поиска объектов откройте оснастку Active Directory Users And Computers, ярлык которой находится в группе программ Administrative Tools. В дереве консоли щелкните правой кнопкой мыши домен или ОП и выберите в контекстном меню команду Find (Найти). Откроется диалоговое окно Find (Поиск).

Примечание Если Вы раскроете контекстное меню объекта Shared folder (Общая папка) и выберете команду Find (Найти), будет запущена функция поиска Windows Explorer, и Вы сможете искать в общей папке файлы и подпапки.

Диалоговое окно Find включает параметры поиска в ГК, позволяющие находить учетные записи, группы и принтеры (рис. 6-8).

Как видите, это окно разбито на несколько секций: основную, вкладку искомого объекта Users, Contacts and Groups (Пользователи, контакты и группы), вкладку Advanced (Дополнительно) и панель результатов.

Основное окно

Назначение большинства элементов основного окна утилиты Find очевидно, однако о списках Find (Найти) и In (в) мы поговорим более подробно. Кроме того, основное окно содержит две вкладки: вкладку искомого объекта и вкладку Advanced (Дополнительно), которые здесь также будут подробно рассмотрены.

Список Find

Содержит типы доступных для поиска объектов. По умолчанию выполняется поиск Users, Contacts, And Groups (Пользователи, контакты и группы).

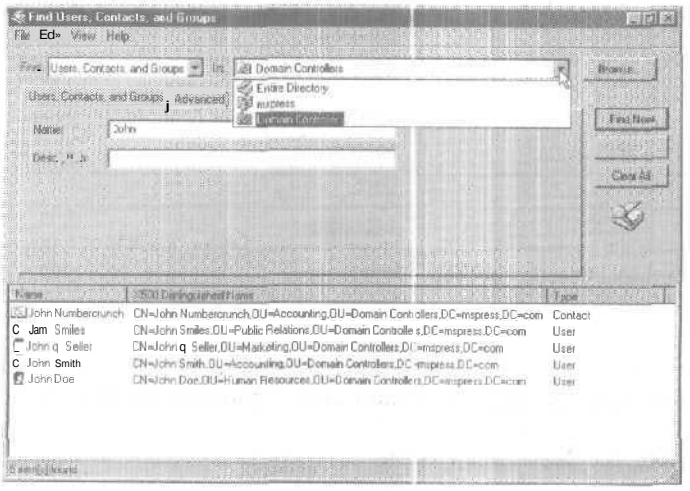


Рис. 6-8. Диалоговое окно Find (Поиск) в оснастке Active Directory Users And Computers (Active Directory — пользователи и компьютеры)

Примечание Заголовок диалогового окна изменяется в зависимости от значения, выбранного в списке Find. Например, если выбрано Organizational Units (Организационные подразделения), заголовок изменится на Find Organizational Units (Поиск: Организационные подразделения).

Список /л

Определяет область поиска. Вы должны выбрать один из вариантов: Active Directory store (Целиком Папка), определенный домен или ОП. По умолчанию указан текущий домен.

Вкладка Users, Contacts and Groups

В поле Name (Имя) вводится имя объекта, а в поле Description (Описание) — его описание. Поиск ведется по комбинации значений обоих полей; разрешается использовать метасимволы.

Вкладка Advanced

Позволяет настроить дополнительные условия поиска, используемые совместно с параметрами на вкладке Users, Contacts, And Groups или самостоятельно. Поиск ведется на основании сведений, указанных на обеих вкладках. Если на вкладке Users, Contacts And Groups условие не введено, результаты будут зависеть только от сведений на вкладке Advanced (Дополнительно).

Вот подробное описание полей вкладки Advanced:

Поле	Описание
Field (Поле)	Список атрибутов, по которым Вы можете вести поиск объекта выбранного типа.
Condition (Условие)	Дополнительные способы дальнейшего сужения поиска по атрибутам. Возможные варианты: Starts With (начинается), Ends With (заканчивается), Is (Exactly) (совпадает), Is Not (не совпадает), Present (присутствует) и Not Present (отсутствует).
Value (Значение)	Значение для указанного в поле Field (Поле) атрибута, используемое для поиска в каталоге. Вы можете искать объект по его атрибуту, только если Вы укажете значение атрибута. Например, чтобы найти пользователей, чье имя начинается с буквы «R», в поле Field надо выбрать First Name (Фамилия), в Condition — Starts With (начинается), а в Value — R.
Список условий поиска	Здесь перечислены все определенные Вами условия поиска. Определив условия в полях Field, Condition и Value, щелкните кнопку Add (Добавить) — условие поиска будет добавлено в окно. Вы вправе добавлять или удалять условия для расширения или сужения области поиска.

Панель результатов

Открывается в нижней части основного окна и представляет результаты поиска, полученные после шелчка кнопки Find Now (Найти) в основном окне. Чтобы добавить или удалить столбцы, отображаемые на панели результатов, выберите в меню View (Вид) команду Choose Columns (Выбрать стобцы).

Изменение значений атрибутов и удаление объектов

Вы вправе изменять значения атрибутов объекта для изменения или добавления информации.

Примечание Не путайте модификацию значений атрибутов объекта с дополнением, удалением, или модификацией объектов или атрибутов в схеме. Изменения схемы постоянны и реплицируются на все контроллеры домена в лесе.

Чтобы изменить значения атрибута, откройте оснастку Active Directory Users And Computers и выберите экземпляр объекта. В меню Action (Действие) выберите команду Properties (Свойства). В диалоговом окне свойств объекта измените нужные атрибуты объекта. Затем внесите поправки в описание объекта, например, модифицируйте объект User, чтобы изменить имя, местоположение и электронный адрес пользователя.

Если объекты больше не нужны, удалите их в целях безопасности: открыв оснастку Active Directory Users And Computers, выделите экземпляр удаляемого объекта, а затем в меню Action (Действие) выберите команду Delete (Удалить).

Перемещение объектов

В хранилище Active Directory можно перемещать объекты, например между ОП, чтобы отразить изменения в структуре предприятия при переводе сотрудника из одного отдела в другой. Для этого, открыв оснастку Active Directory Users And Computers, выделите перемещаемый объект, в меню Action (Действие) выберите команду Move (Переместить) и укажите новое местоположение объекта.

Упражнение 6: управление объектами Active Directory

Сначала найдите объект User, созданный в предыдущем упражнении, а затем переместите его в другое место.

▶ **Задание 1: Найдите учетную запись пользователя в домене**

Найдите объект пользователя Jane. Она была переведена в отдел продаж, поэтому соответствующий ей объект был перемещен в ОП Sales. Вы знаете часть ее телефонного номера и ее имя.

1. Зарегистрируйтесь на Server01 как Administrator с паролем password.
2. Откройте оснастку Active Directory Users And Computers (Active Directory — пользователи и компьютеры).
3. В дереве консоли щелкните microsoft.com.
4. В меню Action (Действие) выберите команду Find (Найти).

   Откроется окно Find Users, Conlacts, And Groups (Поиск: пользователи, контакты и группы).
5. Убедитесь, что в списке Find (Найти) выбрано Users, Contacts, And Groups (Пользователи, контакты и группы) и щелкните кнопку Find Now (Найти).

   Заметьте: объекты User и Group обнаруживаются независимо от их местоположения.
6. Щелкните кнопку Clear All (Очистить все), а затем — кнопку OK чтобы очистить панель результатов поиска.
7. Убедитесь, что в списке In (в) значится домен microsoft.
8. В поле Name (Имя) введите Jane.
9. Перейдите на вкладку Advanced (Дополнительно).
10. Щелкните кнопку Field (Поле), выберите User (Пользователь) и затем щелкните Telephone Number (Номер телефона).

Примечание Если в списке не видно пункта Telephone Number, прокрутите список вниз.

---

11. В поле Value (Значение) наберите 555-12 и щелкните кнопку Add (Добавить).
12. В меню View (Вид) выберите команду Choose Columns (Выбрать столбцы).

    Откроется диалоговое окно Choose Columns (Выбор столбцов).

13. В списке Columns Shown (Отображаемые столбцы) щелкните пункт Description, а затем — кнопку Remove (Удалить).
14. Прокрутите список Columns Available (Доступные столбцы), выберите X500 Distinguished Name (X500 различающееся имя) и щелкните кнопку Add (Добавить).
15. Щелкните кнопку (Ж, чтобы закрыть диалоговое окно Choose Columns.

    В диалоговом окне Find Users, Contacts And Groups отображаются параметры найденного пользователя Jane Doe с типом объекта User (Пользователь) и различающимся именем CN=Jane Doe, CN=Users, DC=microsoft, DC=com.

    Различающееся имя указывает, что пользователь Jane Doe находится в контейнере Users домена microsoft.com.
16. Закройте диалоговое окно Find Users, Contacts And Groups.

▶ **Задание 2: переместите объект**

Переместите объект пользователя Jane Doe из контейнера Users в контейнер Sales.

1. В дереве консоли оснастки Active Directory Users And Computers (Active Directory - пользователи и компьютеры) щелкните Users.

   На правой панели появятся все объекты с типом User (Пользователь) и Security Group (Группа безопасности).
2. На правой панели щелкните объект пользователя Jane Doe.
3. В меню Action (Действие) выберите команду Move (Переместить).

   Откроется одноименное окно.
4. Выделите ОП Sales и щелкните кнопку OK.

   Пользователь Jane Doe переместится из ОП Users в ОП Sales.
5. В дереве консоли щелкните ОП Sales.

   На правой панели появится объект пользователя Jane Doe.
6. Закройте оснастку Active Directory Users And Computers.

Управление доступом к объектам Active Directory

Для контроля доступа к объектам Active Directory применяется объектно-ориентированная модель зашиты, подобная модели защиты NTFS. Каждый объект Active Directory имеет дескриптор безопасности, определяющий, кто имеет право доступа к объекту и тип этого доступа. Windows 2000 использует дескрипторы безопасности для управления доступом к объектам.

Для упрощения администрирования можно сгруппировать объекты с одинаковыми требованиями безопасности в ОП и назначить разрешения доступа для всего ОП и всех объектов в нем.

Управление разрешениями Active Directory

Разрешения Active Directory обеспечивают защиту ресурсов, позволяя управлять доступом к экземплярам объектов или атрибутам объектов и определять вид предоставляемого доступа.

Защита Active Directory

Администратор или владелец объекта должен назначить объекту разрешения доступа еще до того, как пользователи смогут получать доступ к этому объекту. Windows 2000 хранит *список управления доступом* (access control list, ACL) для каждого объекта Active Directory. ACL объекта включает перечень пользователей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

Вы можете задействовать разрешения для назначения административных полномочий конкретному пользователю или группе в отношении ОП, иерархии ОП или отдельного объекта без назначения административных разрешений на управление другими объектами Active Directory.

Разрешения доступа к объекту

Зависят от типа объекта — например, разрешение Reset Password допустимо для объектов User, но не для объектов Computer.

Пользователь может быть членом нескольких групп с разными разрешениями для каждой их них, обеспечивающих разные уровни доступа к объектам. При назначении разрешения на доступ к объекту члену группы, наделенной иными разрешениями, эффективные права пользователя будут складываться из его разрешений и разрешений группы. Например, если ему предоставлено разрешение записи срока истечения учетной записи (Write accountExpires) для объектов User и он входит в группу, у которой есть разрешение на чтение срока истечения учетной записи (Read accountExpires), то фактически этот пользователь будет иметь оба этих разрешения.

Вы можете предоставлять или аннулировать разрешения. Аннулированные разрешения для пользователей и групп приоритетнее любых выданных разрешений. Если Вы запретили пользователю обращаться к объекту, то он не получит доступ к нему даже как член полномочной группы. Аннулировать разрешения следует, только если требуется запретить какое-то действие для конкретного пользователя, входящего в полномочную группу.

Примечание Всегда проверяйте, что все объекты имеют минимум одного пользователя с разрешением Full Control (Полный доступ), иначе некоторые объекты станут недоступны лицам, использующим оснастку Active Directory Users And Computers, включая администратора.

Назначение разрешений Active Directory

Настроить разрешения объектов и их атрибутов позволяет оснастка Active Directory Users And Computers. Назначить разрешения также можно на вкладке Security (Безопасность) диалогового окна свойств объекта.

Для выполнения большинства задач администрирования достаточно стандартных разрешений. Впрочем, Вам могут потребоваться и специальные разрешения. Чтобы их настроить, щелкните на вкладке Security кнопку Advanced (Дополнительно). На вкладке Permissions (Разрешения) щелкните интересующее Вас разрешение, а затем — кнопку View/Edit (Показать/Изменить). Просмотреть разрешения конкретных атрибутов можно на вкладке свойств диалогового окна Permission Entry (Элемент разрешения).

Примечание Не назначайте разрешений отдельным атрибутам объектов — это усложнит администрирование системы. В итоге некоторые объекты Active Directory могут выйти из Вашего поля зрения.

Наследование разрешений

Наследование разрешений в Active Directory упрощает настройку доступа к объектам - Вы можете применить разрешения к дочерним объектам текущего объекта. Для отмены наследования разрешений сбросьте флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект) — дочерние объекты не будут наследовать разрешения своего родитель-

ского объекта, и объект получит лишь те разрешения, которые Вы явно ему назначили. Предотвратить наследование можно на вкладке Security (Безопасность) диалогового окна свойств объекта.

При запрещении наследования можно:

- скопировать ранее унаследованные разрешения — набор новых явных разрешений объекта будет копией разрешений, которые он ранее наследовал от родительского объекта; потом разрешения можно скорректировать явно;
- удалить унаследованные разрешения — Windows2000 удаляетвсе унаследованные разрешения, т. е. для объекта вообще не будут определены разрешения; потом для него можно явно указать любые разрешения.

Делегирование полномочий по управлению объектами

Вы вправе предоставить полномочия управления объектами другим лицам, чтобы они могли самостоятельно администрировать объекты. Эту задачу можно выполнить по-разному, например, с помощью мастера Delegation Of Control (Мастер делегирования управления).

Администратор вправе делегировать такие функции:

- назначение разрешений пользователю или группе на создание или изменение объектов в указанном ОП;
- назначение разрешений пользователю или группе на изменение указанных разрешений для атрибутов объектов, например атрибута сброса паролей для объекта User Account.

Поскольку отслеживать разрешения на уровне ОП легче, чем на уровне отдельных объектов или их атрибутов, проще всего делегировать полномочия, назначая разрешения на уровне ОП.

Например, можно делегировать административные полномочия, предоставив разрешение Full Control (Полный доступ) для ОП соответствующему менеджеру в пределах его ответственности, Это поможет децентрализовать выполнение административных задач, приблизив администратора к месту обслуживания.

Вот некоторые основные правила делегирования полномочий:

- делегируйте права на уровне ОП — этоупрощает отслеживание разрешений; следить за разрешениями для конкретных объектов и их атрибутов затруднительно;
- используйте мастер Delegation Of Control Wizard — он назначает разрешения ряду объектов, включая экземпляры объекта OU и другие встроенные объекты, включая Users и Subnets;
- отслеживайте делегирование полномочий— это поможет Вам эффективно управлять системой безопасности;
- следите за изменениями в организационной структуре предприятия.

Мастер Delegation Of Control

Сопровождает Вас в процессе назначения разрешений на уровне ОП. Специальные разрешения можно настроить вручную.

Для запуска мастера Delegation Of Control (Мастер делегирования управления) откройте оснастку Active Directory Users And Computers, выберите ОП, для которого Вы хотите делегировать административные полномочия, и в меню Action (Действие) щелкните команду Delegate Control (Делегирование управления) (рис. 6-9).

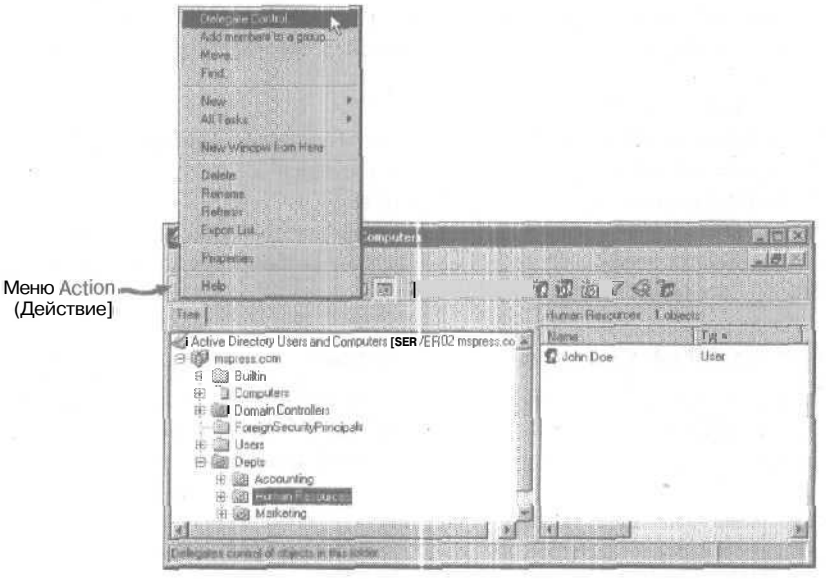


Рис. 6-9. Последовательность запуска мастера Delegation Of Control (Мастер делегирования управления)

Рекомендации по администрированию Active Directory

- В крупных организациях заранее согласовывайте структуру Active Directory с другими администраторами. Вы сможете переместить объекты и позже, но это потребует дополнительных усилий.
- При создании таких объектов Active Directory, как User, заполняйте все атрибуты, важные для Вашей организации. Чем больше атрибутов определено, тем шире возможности поиска.
- Осторожно аннулируйте разрешения. При правильном назначении разрешений Вам, возможно, никогда не понадобится их отменять. Чаще всего аннулирование разрешений свидетельствует об ошибках группирования объектов.
- Всегда проверяйте, чтобы минимум один пользователь имел разрешение Full Control (Полный доступ) для всех объектов Active Directory, иначе объекты могут оказаться недоступны.
- Убедитесь, что уполномоченные пользователи ответственно относятся к возложенным на них функциям и способны правильно их выполнять. В конце концов, как администратор, именно Вы отвечаете за все изменения в системе, и если пользователи, которым Вы доверили выполнение ряда задач в их сети, не справляются, отвечать за их ошибки придется Вам.
- Инструктируйте уполномоченных пользователей. Убедитесь, что они понимают важность их работы и умеют выполнять задачи администрирования.

Резюме

После установки Active Directory Вы можете управлять объектами, хранимыми в каталоге. Перед добавлением объектов в Active Directory надо создать ОП, где они будут содержаться. Вы можете создать ОП на уровне домена, контроллера домена или внутри другого ОП; при этом **Вы** должны обладать соответствующими разрешениями. Управление объектами Active Directory включает их поиск, изменение, перемещение и удаление. Эти задачи выполняются в оснастке Active Directory Users And Computers (Active Directory — пользователи и компьютеры), ярлык которой расположен в программной группе Administrative Tools (Администрирование). Еще один аспект администрирования Active Directory — управление доступом к объектам каталога. Разрешения Active Directory обеспечивают защиту ресурсов, позволяя контролировать доступ к индивидуальным объектам и их атрибутам, а также вид доступа. Кроме того, Вы можете делегировать полномочия администрирования объектов другим лицам для выполнения административных задач в отношении указанных объектов.

Закрепление материала

? j Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Каково назначение файла Ntdis.dit?

2. Опишите требование для размещения SYSVOL?

3. Каково назначение SYSVOL? Назовите единственное требование для размещения SYSVOL на диске.

4. В чем разница между атрибутом и значением атрибута? Приведите примеры.

5. В чем разница между изменением объекта и изменением атрибута экземпляра объекта?

6. Надо разрешить менеджеру отдела продаж создавать, изменять и удалять учетные записи сотрудников его отдела. Как это сделать?

7. Что такое глобальный каталог и каково его назначение?

ГЛАВА 7

Администрирование Microsoft Windows 2000 Server

В этой главе

Эта глава посвящена администрированию Microsoft Windows 2000 Server. На первом занятии изучается консоль управления Microsoft Management Console (MMC) — основной инструмент администрирования Windows 2000 и других продуктов Microsoft, например комплекта BackOffice. В остальной части главы рассмотрены конкретные административные задачи: создание учетных записей пользователей групп и внедрение групповой политики.

Прежде всего

Для выполнения заданий Вам потребуется:

- Windows 2000 Server;
- средства администрирования Active Directory;
- выполнить все упражнения предыдущих глав.

Занятие 1. Использование Microsoft Management Console

Одно из основных средств управления Windows 2000 — консоль MMC — обеспечивает стандартный способ создания, сохранения и открытия средств администрирования с помощью встраиваемых в нее управляющих приложений — *оснасток* (snap-ins).

Изучив материал этого занятия, Вы сможете:

- ✓ описать функции и компоненты MMC, включая оснастки и настройку консоли;
- ✓ создать пользовательскую консоль MMC.

Продолжительность занятия — около 45 минут.

Среда MMC

MMC представляет собой общий интерфейс для приложений управления. Консоль MMC способна работать под Windows 2000/NT 4.0/98/95.

MMC лишь обеспечивает универсальную среду для оснасток — средств, поддерживающих действительные возможности управления. Среда MMC обеспечивает прозрачную интеграцию разных оснасток, даже от разных изготовителей. Администраторы могут создавать средства, включающие многочисленные оснастки, и затем сохранять их для последующего применения или совместного использования с другими администраторами.

MMC позволяет:

- **выполнять большинство административных задач только с помощью MMC** — консоль способна экономить время за счет использования одного интерфейса вместо нескольких;
- **централизовать администрирование** — MMC позволяет выполнять большинство административных задач с одного компьютера;
- **использовать большинство оснасток для удаленного администрирования** — не все оснастки способны выполнять удаленное администрирование, поэтому если оснастка может работать с удаленным компьютером, Windows 2000 выдает соответствующее сообщение;
- **создать пользовательскую консоль** — MMC обеспечивает создание специализированных консолей, содержащих все или часть оснасток; эти пользовательские консоли затем распределяются в группы поддержки для делегирования административных задач.

Примечание MMC 1.1 поддерживала только одну оснастку, а MMC 1.2 в Windows 2000 — несколько оснасток в одном окне консоли.

Окно MMC

Пользовательский интерфейс MMC напоминает Windows Explorer. Компоненты консоли MMC содержатся в окне MMC, в котором имеется меню и панель инструментов, содержащая команды открытия, создания и сохранения консоли MMC. Это меню и панель инструментов называются *главное меню* (main menu bar) и *главная панель инструментов* (main toolbar). В нижней части окна — строка состояния, а вдоль верхней части панели подробных сведений — строка описания. Родительское окно включает дочерние окна, также консоли MMC.

MMC можно сконфигурировать для работы с мощными средствами управления (рис. 7-1). MMC представляет данные в удобном виде, заметно облегчающем работу администраторов.

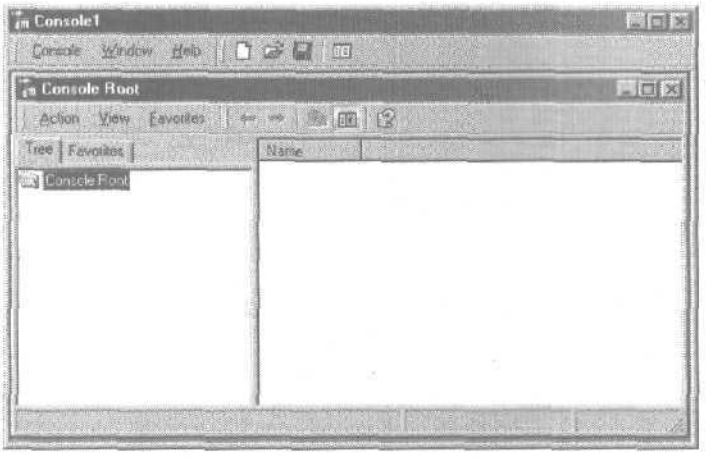


Рис. 7-1. Окно MMC

Консоли MMC

Консоль - это набор оснасток. Консоли сохраняются в файлах с расширением *.msc. Каждый файл консоли в интерфейсе MMC выглядит как дочернее окно. Файл консоли MMC включает дерево, представляющее иерархию оснасток в файле. Все параметры оснастки сохраняются и восстанавливаются при открытии файла, даже если он открывается на другом компьютере или в сети.

Окно консоли

Окно консоли (дочернее окно), являющееся интерфейсом для файла консоли MMC, можно просматривать в разных видах. Любое такое окно включает командную панель, дерево консоли (левая панель) и окно подробных сведений (правая панель). На рис. 7-2 окно консоли на заднем плане содержит три оснастки, а на переднем плане Вы видите дочернее окно консоли Computer Management (Управление компьютером).

Панель команд включает раскрывающиеся меню и кнопки.

Меню	Описание
Action (Действие)	Создает, удаляет и изменяет элементы, управляемые оснасткой, Конкретные функции зависят от того, какая оснастка активна.
View (Вид)	Конфигурирует экран оснастки.
Favorites (Избранное)	Организует оснастки или их узлы или управляет папками, содержащими объекты MMC. Затем эти компоненты появляются на вкладке Favorites. Вкладка Favorites изображена на рис. 7-1 и 7-2 за вкладкой Tree (Структура).

Примечание Для некоторых объектов дерева консоли появляются дополнительные элементы раскрывающегося меню. Например, на рис. 7-2 видно, что при выборе в дереве консоли пункта System Information появляется раскрывающееся меню Tools.

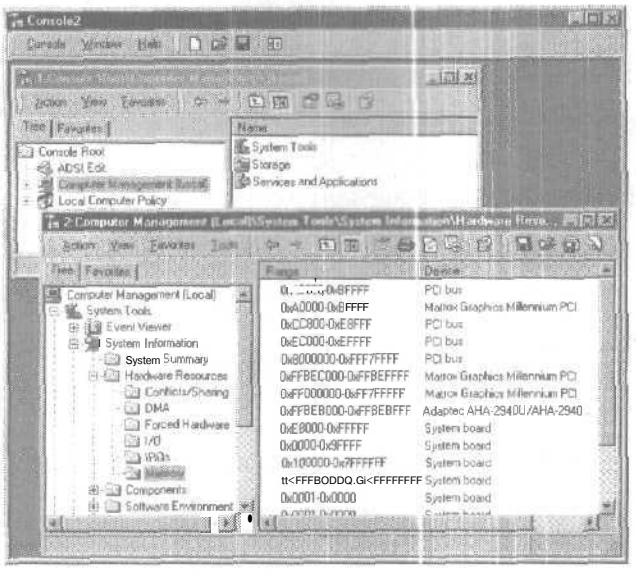


Рис. 7-2. **Консоль MMC, включающая несколько оснасток и дочернее окно**

Дерево консоли организует оснастки — части консоли MMC. Такая организация позволяет легко найти конкретную оснастку. Элементы, добавляемые к дереву, появляются в корне консоли. Дерево отображает пространство имен инструмента и древовидный список всех видимых узлов, каждый из которых представляет управляемый объект, задачу или вид. Дерево консоли не обязательно присутствует на экране во всех видах.

Каждое окно подробных сведений, называемое панелью результатов, реагирует на выбор узла в дереве консоли. Обычно оно отображает список содержимого папки, а иногда — связанный с выбранным в дереве узлом вид на основе Web-страницы или управляющего элемента ActiveX.

Типы консолей MMC

Консоли MMC бывают двух типов: пользовательские и преднастроенные.

Пользовательские консоли MMC

Одну или несколько оснасток или их частей можно объединить для создания пользовательской консоли, которую затем можно применять для централизованного администрирования. MMC позволяет администраторам:

- сохранять пользовательские MMC для повторного применения;
- распределять их другим администраторам и совместно с ними работать с пользовательскими MMC;
- с помощью пользовательских MMC централизовать и объединять административные задачи с любого компьютера.

Для создания собственных пользовательских консолей MMC можно объединять готовые оснастки с другими — от независимых производителей ПО, выполняющими связанные задачи. Создав пользовательскую MMC, Вам не придется переключать различные программы или предварительно настроенные MMC, поскольку все нужные оснастки будут размещены в Вашей консоли.

По умолчанию Windows 2000 сохраняет файлы пользовательских консолей в папке My Administrative Tools (Администрирование) с расширением *.msc. Если этой папки нет, Windows 2000 создает ее. Windows 2000 сохраняет содержимое папки My Administrative Tools отдельно для каждого пользователя.

Примечание Подробнее о создании консолей MMC см. документ \chapt07\articles\microsoft management console.doc на прилагаемом компакт-диске.

Преднастроенные MMC

С Windows 2000 автоматически устанавливаются Преднастроенные консоли MMC. Они включают оснастки, обычно используемые для администрирования. Авторские консоли MMC неизменяемы, добавить к ним дополнительные оснастки нельзя.

Преднастроенные консоли MMC содержат только одну оснастку, обеспечивающую выполнение соответствующего набора административных задач. Консоли функционируют в режиме пользователя, что означает невозможность их изменения, сохранения или добавления дополнительных оснасток. Действие режима пользователя можно определить по отсутствию таких меню MMC, как Console (Консоль), Window (Окно) и Help (Справка), и объектов панели инструментов MMC. Кроме того, консоли MMC иногда добавляются при установке дополнительных компонентов. Например, при установке службы Domain Name System (DNS) Windows 2000 устанавливает консоль DNS.

Примечание Для выбора предварительно настроенных консолей MMC служит меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование).

Набор установленных консолей MMC зависит от версии Windows 2000 и установленных компонентов. Windows 2000 Server и Windows 2000 Professional имеют различные преднастроенные консоли MMC, появляющиеся в меню Administrative Tools. Для удаленного администрирования к Windows 2000 Professional добавляются включенные в Windows 2000 Server Преднастроенные консоли M MC. Все административные инструменты Windows 2000 Server легко добавить, установив пакет Adminpak.msi с установочного компакт-диска Windows 2000 Server.

Оснастки

Оснастка — это единица функций управления и минимальная единица расширения консоли. Оснастка расширяет консоль MMC, позволяя выполнять различные административные задачи. Оснастки бывают двух типов: изолированные и расширения. Рис. 7-3 показывает диалоговое окно Add/Remove Snap-In (Добавить/Удалить оснастку), вызываемое из меню Console. Оба типа оснасток добавляются из этого окна.

Изолированная оснастка

Обычно называется просто оснастка. Используйте изолированные оснастки для администрирования Windows 2000. Каждая обеспечивает одну функцию или связанный набор функций. Windows 2000 Server включает стандартный набор оснасток, больший, чем в Windows 2000 Professional.

Расширение оснастки

Обычно называется просто расширение. Обеспечивает дополнительные административные функциональные возможности для других оснасток. Расширения созданы для работы с одной или несколькими изолированными оснастками на основе функции изолированной оснастки. При добавлении расширения Windows 2000 выводит на экран только расширения, совместимые с изолированной оснасткой. Windows 2000 помещает расширения в изолированную оснастку. Некоторые оснастки, например Event Viewer, могут действовать и как оснастка, и как расширение.

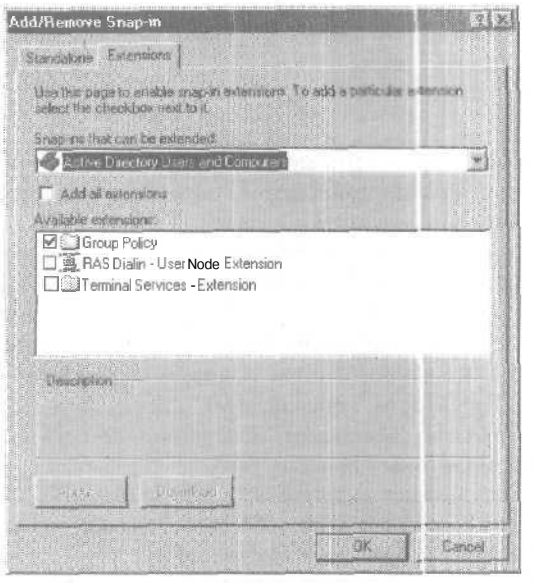


Рис. 7-3. **Диалоговое окно Add/Remove Snap-In (Добавить/Удалить оснастку), иллюстрирующее настройку расширений на вкладке Extensions (Расширения)**

Расширения могут обеспечивать ряд функциональных возможностей. Некоторые действительно расширяют пространство имен консоли; так, System Information (Сведения о системе) добавит к пространству имен системную информацию для каждого компьютера в пространстве имен. Другие просто расширяют контекстные меню или увеличивают число специальных мастеров.

Многие оснастки реализуют изолированную функциональность и способны расширять другие оснастки. Например, оснастка Event Log (Просмотр событий) читает сведения журналов событий компьютеров. Если в консоли есть объект Computer Management (Управление компьютером), Event Log автоматически расширяет каждый экземпляр этого объекта и позволяет просмотреть журналы событий компьютера. В то же время Event Log также работает в изолированном (Stand-alone) режиме — вне узла Computer Management, как самостоятельный узел.

Параметры **консоли**

Консоли MMC содержат оснастки, выполняющие определенные задачи. Действия MMC задают параметры консоли. Ее параметры позволяют создать MMC для выполнения задач с компьютеров других администраторов. Режим консоли определяет функциональные возможности MMC для того, кто работает с сохраненной MMC, Консоль доступна в двух режимах: авторском и пользовательском.

Авторский режим

При сохранении MMC в авторском режиме разрешается полный доступ ко всем функциональным возможностям MMC, включая изменение консоли. Сохраненная в авторском режиме консоль MMC позволяет:

- добавлять или удалять оснастки;
- создавать новые окна;

- видеть все части дерева консоли;
- сохранять консоли MMC.

Примечание По умолчанию все новые MMC сохраняются в авторском режиме.

Пользовательский режим

Если планируется распространять MMC другим администраторам, сохраните ее в этом режиме. Пользователи тогда не смогут добавлять к ней оснастки, удалять их из нее и сохранять консоль.

Пользовательские режимы могут быть трех типов, обеспечивающих разные уровни доступа и функциональных возможностей:

Тип пользовательского режима	Описание
Full Access (Полный доступ)	Позволяет пользователям переходить от одной оснастки к другой, открывать новые окна и получать доступ ко всем частям дерева консоли.
Limited Access, Multiple Windows (Ограниченный доступ, многооконный)	Запрещает пользователям открывать новые окна или получать доступ ко всем частям дерева консоли, но разрешает им просмотр многочисленных окон в консоли.
Limited Access, Single Window (Ограниченный доступ, однооконный)	Запрещает пользователям открывать новые окна или получать доступ ко всем частям дерева консоли и разрешает им просмотр только одного окна в консоли.

Упражнение 1: навигация и создание пользовательской консоли MMC

Вы поработаете с одной из консолей MMC Windows 2000 Server, а затем создадите пользовательскую MMC.

► Задание 1: используйте существующую консоль MMC

Вы используете консоли MMC, поставляемые с Windows 2000 Server. Выполняйте упражнение с Server01.

1. Зарегистрируйтесь на ServerOl как Administrator (Администратор) с паролем password.
2. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык Event Viewer (Просмотр событий).

   Откроется окно консоли Event Viewer, обеспечивающее доступ к содержимому файлов службы Event Log (Журнал событий) на Вашем компьютере. Event Viewer применяется для наблюдения за действиями аппаратных средств и ПО.

   Заметьте: приведено несколько журналов регистрации. При установке Windows 2000 Server всегда появляются Application log (Журнал приложений), Security log (Журнал безопасности) и System log (Журнал системы). При добавлении дополнительных служб появляются дополнительные журналы регистрации. Вы увидите журнал Directory Service (так как ServerOl настроен для работы службы каталогов), журнал DNS Server (так как сервер настроен для работы в качестве сервера DNS) и журнал File Replication Service (Служба репликации файлов), так как на ServerOl запускается FRS.
3. Закройте консоль Event Viewer (Просмотр событий).

► **Задание 2: создайте и задействуйте пользовательскую консоль MMC**

Вы создадите консоль MMC, настроите ее под пользователя и подтвердите время последнего запуска Вашего компьютера. Вы также добавите оснастки с расширениями.

1. В меню Start (Пуск) выберите команду Run (Выполнить),
2. В поле Open (Открыть) введите mmc и щелкните кнопку OK.
3. Разверните окно Consolel на весь экран.
4. Разверните дочернее окно Console Root.
5. В меню Console выберите команду Options (Параметры) для просмотра текущих параметров.

   Откроется диалоговое окно Options (Параметры).
6. В каком режиме работает консоль?
7. Проверьте, что в списке Console Mode (Режим консоли) выбран авторский режим, и щелкните кнопку OK.
8. В меню Console выберите команду Save (Сохранить).

   Откроется диалоговое окно Save As (Сохранить как).

   Пользовательские консоли по умолчанию располагаются в папке Administrative Tools (Администрирование). Для текущего вошедшего в систему пользователя это соответствует программной группе Administrative Tools (Администрирование).
9. В поле File Name (Имя файла) введите All **Events** и щелкните кнопку Save.

   Название Вашей консоли появится в строке заголовка MMC.
10. Чтобы убедиться, что консоль сохранена по верному пути, в меню Console выберите команду Exit (Выход).
11. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык All Events.msc.

    Откроется сохраненная ранее консоль All Events.
12. В меню Console выберите команду Add/Remove Snap-In (Добавить/удалить оснастку).

    Откроется диалоговое одноименное окно с выбранной вкладкой Stand-Alone (Изолированная оснастка). Загруженных оснасток в настоящий момент нет.
13. Щелкните кнопку Add (Добавить).

    Откроется диалоговое окно Add Stand Alone Snap-In (Добавить изолированную оснастку).
14. Выбрав в перечне оснасток Event Viewer, щелкните кнопку Add.

    Откроется диалоговое окно Select Computer (Выбор компьютера), позволяющее выбрать управляемый компьютер.

    Заметьте, что Event Viewer можно добавить к локальному компьютеру, на котором Вы работаете, или к удаленному, если локальный — часть сети.
15. Убедитесь, что в диалоговом окне Select Computer (Выбор компьютера) выбран переключатель Local Computer (Локальный компьютер), и шелкните кнопку Finish (Готово).
16. В диалоговом окне Add Stand Alone Snap-In щелкните кнопку Close (Закрыть), а в окне Add/Remove Snap-In — OK.

    В дереве консоли появится узел Event Viewer (Local) [Просмотр событий (локальных)].

Совет Чтобы увидеть полное ими папки, перетащите границу между окнами консоли вправо.

---

17. В дереве консоли All Events раскройте узел Event Viewer (Local) и щелкните пункт System (Система).

    На правой панели появится перечень зарегистрированных системных событий,

18. Дважды щелкните самое последнее информационное событие, в столбце Source которого значится eventlog.

    Служба регистрации событий Event Log запускается вместе с системой. Дата и время ее запуска примерно соответствуют дате и времени запуска системы.
19. Чтобы закрыть диалоговое окно Event Properties (Свойства: Событие), щелкните кнопку OK.
20. В меню Console выберите команду Exit, чтобы закрыть консоль All Events.

    Появится запрос сохранить настройку консоли All Events.
21. Щелкните кнопку No (Нет).
22. В меню Start (Пуск) выберите команду Run (Выполнить).
23. В поле Open (Открыть) введите **mmc** и щелкните кнопку OK.
24. Разверните окна Console1 и Console Root.
25. В меню Console выберите команду Add/Remove Snap-In.

    Откроется одноименное окно с выбранной вкладкой Stand-Alone (Изолированная оснастка). Добавьте в корень консоли оснастку.
26. Щелкните кнопку Add (Добавить).

    Все перечисленные оснастки являются изолированными.
27. В диалоговом окне Add Stand Alone Snap-In выберите Computer Management и щелкните кнопку Add (Добавить).

    Откроется диалоговое окно Computer Management,
28. Убедитесь, что выбран переключатель Local Computer (Локальный компьютер) и щелкните кнопку Finish (Готово).
29. Щелкните кнопку Close (Закрыть).

    В списке добавленных оснасток появится Computer Management.
30. Щелкните кнопку OK в диалоговом окне Add/Remove Snap-In.

    В корне консоли появится узел Computer Management (Управление компьютером).
31. Раскрыв этот узел, просмотрите доступные функции, и раскройте узел System Tools (Служебные программы).

Примечание **Не** используйте сейчас какой-либо из этих инструментов.

Заметьте: доступны несколько расширений, в том числе Device Manager (Диспетчер устройств) и System Information (Сведения о системе). Функциональные возможности оснастки можно ограничить, удалив расширения.

32. В меню Console (Консоль) выберите команду Add/Remove Snap-In.

    Откроется одноименное диалоговое окно.
33. Щелкните Computer Management (Local), затем — вкладку Extensions (Расширения).

    Откроется список доступных расширений, содержащихся в оснастке Computer Management.
34. Выберите в списке оснастку Computer Management и сбросьте флажок Add All Extensions (Добавить все расширения). Затем в списке Available Extensions (Доступные расширения) сбросьте флажок Device Manager Extension (Расширение диспетчера устройств) и System Information Extension (Расширение сведений о системе).
35. Щелкните кнопку OK.

    Откроется окно консоли.

36. Чтобы убедиться, что Device Manager и System Information удалены, раскройте узлы Computer Management и System Tools (Служебные программы).

Примечание **Не используйте** сейчас **один из этих инструментов.**

37. В меню Console (Консоль) выберите команду Options (Параметры).

    Откроется диалоговое окно Options (Параметры).

38. В списке Console Mode (Режим консоли) выберите одно окно User Mode — Limited Access single window (Пользовательский — ограниченный доступ, однооконный).
39. Пометив флажок Do Not Save Changes To This Console (Не сохранять изменения для этой консоли), щелкните кнопку OK.
40. Закройте консоль.

    MMC предложит подтвердить сохранение настройки консоли.

41. Щелкните кнопку Yes (Да).

    Откроется диалоговое окно Save As (Сохранить как).

42. В поле File Name (Имя файла) введите **ComputerMgmt** Restricted и щелкните кнопку Save (Сохранить).
43. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык ComputerMgmt Restricted.

    Заметьте, что пользовательская консоль открывается в одном окне.

44. Закройте консоль.

    Обратите внимание: запрос на сохранение консоли не выдается.

Резюме

MMC — одно из основных административных средств управления Windows 2000 Server, обеспечивающее стандартный способ их создания, сохранения и открытия. Эти средства — консоли MMC — включают одну или несколько оснасток, которые представляют собой приложения управления для выполнения административных задач. По умолчанию Windows 2000 сохраняет файлы пользовательских MMC с расширением *.msc в папке Administrative Tools (Администрирование). Каждая MMC имеет дерево консоли, которое отображает иерархическую организацию содержащихся в ней оснасток и окно подробных сведений со списком содержимого активной оснастки. Оснастки бывают двух типов: изолированные и расширения. Первый обеспечивает одну функцию или связанный набор функций. Второй добавляет к изолированной оснастке функциональные возможности администрирования. Каждую консоль можно настроить для работы в пользовательском или авторском режимах, Первый не разрешает другим пользователям добавлять или удалять оснастки из консоли или сохранять консоль. Второй разрешает полный доступ ко всем функциональным возможностям MMC. Консоли можно настраивать и распространять среди пользователей в сети.

Замятие 2, Администрирование учетных записей пользователей

Для регистрации пользователя в домене (и доступа к ресурсам сети) или в локальной системе (и доступа к локальным ресурсам) создается *учетная запись пользователя* (user accounts) — набор уникальных реквизитов, идентифицирующих его для Windows 2000. Учетная запись включает имя пользователя и, если требуется, пароль для регистрации в системе, указывает его принадлежность к группам и определяет его привилегии и разрешения на использование компьютера и сети и на доступ к ресурсам. Каждый пользователь, регулярно работающий в сети, имеет учетную запись.

Изучив материал этого занятия, Вы сможете:

- ✓ описать роль и назначение учетных записей пользователей;
- ✓ планировать и создавать учетные записи пользователей;
- ✓ администрировать учетные записи, включая настройку их параметров.

Продолжительность занятия — около 60 минут.

Учетные записи пользователей Windows 2000

Windows 2000 поддерживает два типа учетной записи пользователя: доменную и локальную. Первая позволяет пользователю войти в домен для доступа к сетевым ресурсам, вторая — войти в систему определенного компьютера для получения доступа к ресурсам этого компьютера.

Кроме того, Windows 2000 предоставляет встроенные учетные записи, применяемые для выполнения административных задач или доступа к сетевым ресурсам.

Доменные учетные записи

Позволяют войти в домен и получить доступ к ресурсам сети. При входе пользователь вводит свой пароль и имя. Эта информация позволяет Windows 2000 аутентифицировать его и создать маркер доступа, содержащий сведения о пользователе и параметрах безопасности. Маркер доступа идентифицирует пользователя для компьютеров с Windows 2000, к ресурсам которых он пытается получить доступ. Windows 2000 предоставляет маркер доступа на время выполнения входа.

Учетная запись пользователя создается в организационном подразделении (ОП) в реплике хранилища Active Directory (именуемом каталогом) на контроллере домена. Контроллер домена реплицирует информацию о новой учетной записи пользователя на все контроллеры домена в домене.

После репликации информации о новой учетной записи пользователя все контроллеры данного домена могут аутентифицировать его при входе.

Примечание Репликация информации о новой учетной записи пользователя домена на все контроллеры домена занимает несколько минут, что может помешать пользователю сразу войти в систему по только что созданной доменной учетной записи. Информация Active Directory в пределах сайта автоматически реплицируется каждые 5 минут.

Локальные учетные записи

Разрешают пользователям входить в систему и получать доступ к ресурсам только на том компьютере, на котором создана локальная учетная запись. При создании локальной учетной записи Windows 2000 создает ее только в БД безопасности данного компьютера. Windows 2000 не реплицирует информацию о локальной учетной записи на контроллеры домена. После создания локальной учетной записи компьютер использует свою локальную БД безопасности для аутентификации локальной учетной записи, что позволяет пользователю войти в систему данного компьютера.

Встроенные учетные записи пользователей

Windows 2000 автоматически создает несколько встроенных учетных записей, из которых чаще всего применяются Администратор (Administrator) и Гость (Guest). ОС не позволяет удалять встроенные учетные записи или отключать запись Administrator, хотя встроенные учетные записи можно переименовывать.

Учетная запись Administrator

Применяется для управления общей конфигурацией компьютера или домена, например для создания и изменения учетных записей пользователей и групп, управления политикой безопасности, создания принтеров и предоставления учетным записям разрешений доступа к ресурсам. Если **Вы** администратор, создайте учетную запись пользователя для выполнения неадминистративных задач. Применяйте учетную запись Administrator только для выполнения административных задач. Для удобства используйте команду runas для работы в контексте более привилегированной учетной записи после входа в систему с менее привилегированной. Например, если Вы вошли в систему со стандартными правами, для работы с консолью MMC в качестве администратора выполните команду:

```
runas user:<имя_домена>\<учетная_запись_администратора> mmc
```

Если учетная запись администратора в домене microsoft.com — Administrator введите:

```
runas /user:microsoft\administrator mmc
```

Совет Переименуйте встроенную учетную запись Administrator для обеспечения безопасности. Используйте имя, явно не указывающее на административные полномочия. Это затруднит взлом административной учетной записи, поскольку злоумышленники не будут знать ее имя. Затем создайте учетную запись Administrator, которая вообще не будет иметь прав в системе.

Учетная запись Guest

Позволяет случайным пользователям войти в систему и получить временный доступ к ресурсам.

Примечание **Учетная запись** Guest **по умолчанию отключена. Включайте ее только в** сетях с **низким** уровнем **безопасности и** всегда назначайте ей **пароль.**

Планирование новых учетных записей пользователей

Планируя и организуя информацию для учетных записей пользователей, можно упростить процесс их создания. Следует планировать:

- правила именования учетных записей пользователей;
- требования к паролям;

- параметры учетных записей, например время входа в систему, компьютеры, с которых в нее можно войти, и срок действия учетной записи.

Правила именования

Определяют порядок идентификации пользователей в домене. Постоянные правила именования помогут Вам и Вашим пользователям запомнить пользовательские имена входа в систему и найти их в списке. Вот некоторые вопросы, рассматриваемые при определении правил именования:

Предмет рассмотрения	Объяснение
Уникальные регистрационные имена пользователей	Регистрационные имена пользователей домена должны быть уникальны в пределах каталога и внутри ОП, где создаются доменные учетные записи. Локальные учетные записи должны быть уникальны в пределах компьютера.
Максимум 20 символов	Регистрационное имя может содержать не более 20 символов прописных или строчных букв. Поле ввода принимает более 20 символов, но Windows 2000 распознает только первые 20.
Недопустимые символы	" / \ [ ] : ; | = , + * ? < >
Регистрационные имена не чувствительны к регистру	Для создания уникальных учетных записей можно использовать комбинацию специальных и алфавитно-цифровых символов. Регистрационные имена не чувствительны к регистру, хотя и сохраняют его.
Сотрудники с одинаковыми именами	Для различения одинаковых имен можно использовать имя и первую букву фамилии и затем добавить разное количество букв фамилии. Для различения двух сотрудников с именем John Doe можно выбрать имена Johnd и Johndo. Можно добавить в имя и цифру, например, Johndl и Johnd2.
Тип сотрудника	Иногда по учетным записям пользователей полезно идентифицировать временных сотрудников. Например, для идентификации временных сотрудников можно ввести букву T и дефис перед регистрационным именем входа в систему: T-Johnd. Или можно использовать заключенную в скобки пояснительную фразу, например John Doe (Temp).
Имена учетных записей служб	Для работы многих фоновых служб требуются учетные записи. Добавьте к именам таких учетных записей аббревиатуру, например svc.

Требования к паролю

В целях защиты доступа к домену или компьютеру каждый пользователь должен иметь пароль.

Для паролей существуют следующие правила.

- Для предотвращения несанкционированного доступа к учетной записи Administrator присваивайте пароль для этой учетной записи.
- Определите, будут ли администратор или пользователи контролировать пароли. Вы можете присвоить уникальные пароли для учетных записей пользователей и запретить

пользователям изменять их или разрешить им ввести свои пароли при первом входе в систему. В большинстве случаев контролировать пароли следует пользователям.

- Используйте пароли, которые сложно разгадать. Избегайте паролей, содержащих явные ассоциации, например, имена членов семьи.
- Пароль может содержать до 128 символов, минимальная рекомендуемая длина — 8 символов.
- Используйте прописные и строчные буквы, цифры и допустимые специальные символы. Недопустимые символы перечислены в приведенной выше таблице.

Параметры учетных записей

Определите время, когда пользователь может входить в сеть, и компьютеры, с которых это можно делать. Установите сроки действия учетных записей временных пользователей.

Время входа

Для контроля за входом пользователя на домен задайте часы входа в систему — срок, в течение которого пользователи могут работать в сети. По умолчанию Windows 2000 разрешает доступ в любой день 24 часа в сутки. Можно разрешить вход только в рабочее время. Установка времени входа сокращает срок, в течение которого учетная запись открыта для несанкционированного доступа.

Компьютеры, с которых пользователи могут входить в систему

По умолчанию пользователи могут входить в домен с любого компьютера домена. Потребуйте, чтобы пользователи входили в домен только с их собственных компьютеров. Это предотвратит их доступ к конфиденциальной информации на других компьютерах.

Примечание Если отключить NetBIOS поверх TCP/IP, Windows 2000 не сможет определить компьютер, с которого осуществлен вход в систему, и Вы не сможете ограничить вход пользователей определенными компьютерами. Дело в том, что NetBT ограничивает доступ по имени компьютера, а не по MAC-адресу.

Срок действия учетной записи

Определите, задавать ли срок действия учетной записи пользователя. Если да. то для отключения учетной записи при прекращении доступа к сети установите дату окончания действия учетной записи пользователя. Для временных сотрудников установите срок действия учетных записей в соответствии с датой окончания их контрактов.

Создание учетных записей пользователей

Можно создать два типа учетных записей пользователей: доменные и локальные.

Создание доменных учетных записей

Для этого служит оснастка Active Directory Users And Computers (Active Directory — пользователи и компьютеры). Учетная запись пользователя домена создается на первом доступном для MMC контроллере домена и затем тиражируется на все контроллеры домена.

Совет Можно быстро создать большое количество учетных записей пользователей, применив WSH-сценарии. Подробнее о WSH (Windows Script Host) — в справочной системе Windows 2000 Server в подразделе Windows Script Host (Сервер сценариев Windows) раздела Automating Administrative Tasks (Автоматическое выполнение административных задач).

Оснастка Active Directory Users And Computers

Позволяет создавать доменные учетные записи (рис. 7-4).

Для создания **новой учетной записи выберите ОП. Учетную запись пользователя домена можно создать в ОП** Users **(по умолчанию) или в других ОП домена.**

Для создания **доменной** учетной **записи откройте оснастку Active Directory** Users And **Computers и выберите ОП** Users. **В меню Action (Действие)** выберите New (Создать), а затем **— команду** User **(Пользователь)** (рис.7-4). **Введите сведения о пользователе в** диалоговом **окне New Object** — User **(Новый объект — пользователь).**

При создании **доменной учетной записи поле** User **Logon** Name **(Имя** входа пользователя) **по умолчанию относится к домену, в котором создается запись** (рис.7-4). **Можно,** однако, **выбрать любой домен, в котором Вам разрешено** создавать доменные **учетные записи.**

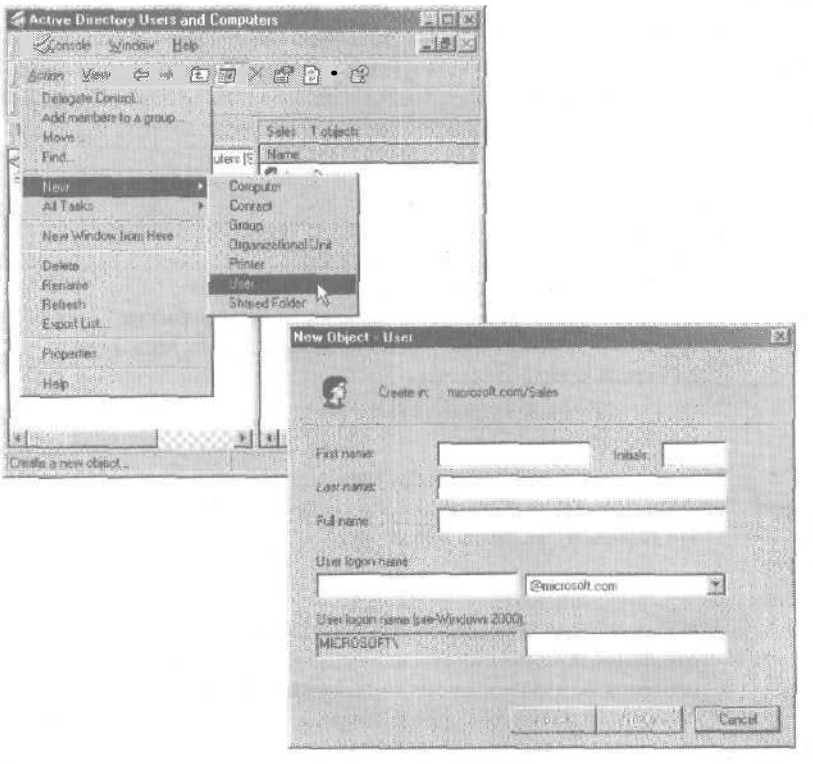


Рис. 7-4. Открытие диалогового окна New Object — User (Новый объект — пользователь) в оснастке Active Directory Users And Computers (Active Directory — пользователи и компьютеры)

Параметры доменной **учетной записи таковы:**

Параметры	Описание
First Name (Имя)	**Имя пользователя.**
Last Name **(Фамилия)**	**Фамилия пользователя.**
Full Name (Полное имя)	**Имя и фамилия** пользователя. **При вводе информации в поля** First Name или **Last Name** Windows 2000 **автоматически заполняет** это поле. Windows 2000 **отображает имя пользователя в ОП, к которому относится его учетная** запись.

(окончание)

Параметры	Описание
User Logon Name (имя входа пользователя)	Уникальное имя пользователя для входа в систему, созданное на основе правил именования. Оно требуется в обязательном порядке и должно быть уникальным в каталоге.
User Logon Name (pre-Windows 2000) [Имя входа пользователя (пред-Windows 2000)]	Уникальное имя пользователя, применяемое для входа в систему клиентов низшего уровня (пред-Windows 2000), например Windows NT 4.0/3.51. Оно требуется в обязательном порядке. и должно быть уникальным в домене.

Настройка требований к паролю

При добавлении новой учетной записи для пользователя можно ввести пароль. В диалоговом окне New Object — User щелкните кнопку Next (Далее), чтобы открыть второе диалоговое окно New Object — User. Здесь задаются параметры пароля для доменной учетной записи. Вводить пароль для пользователя не обязательно, но тогда пользователь будет входить в домен без пароля.

Параметры пароля таковы:

Параметры	Описание
Password (Пароль)	Пароль служит для аутентификации пользователя. Для обеспечения большей безопасности пароль следует присваивать всегда. Заметьте: при наборе пароль представлен на экране в виде звездочек.
Confirm Password (Подтверждение)	Чтобы убедиться в правильности ввода пароля, подтвердите его, набрав еще раз.
User Must Change Password At Next Logon (Потребовать смену пароля при следующем входе в систему)	Выберите этот параметр, если хотите, чтобы пользователь изменил свой пароль при первом входе в систему. Это гарантирует, что пароль будет знать только он.
User Cannot Change Password (Запретить смену пароля пользователем)	Выберите этот параметр, если несколько человек пользуются одной доменной учетной записью (например, Guest) или для контроля за паролями учетных записей. Этот параметр обычно задают для контроля паролей учетных записей фоновых служб.
Account Is Disabled (Отключить учетную запись)	Служит для запрещения этой учетной записи, например для нового сотрудника, еще не приступившего к работе.
Password Never Expires (Срок действия пароля не ограничен)	Выберите этот параметр, если пароль не должен меняться, например, для доменной учетной записи, которая понадобится какой-либо программе или службе Windows 2000. Данный параметр переопределяет параметр User Must Change Password At Next Logor (Потребовать смену пароля при следующем входе в систему). Если выбраны оба, Windows 2000 автоматически снимает флажок User Must Change Password At Next Logon.

Примечание Всегда требуйте, чтобы новые пользователи изменяли свои пароли при первом входе в систему. Это заставит их применять пароли, известные только им. Для усиления безопасности в сетях при помощи комбинации цифр и букв создайте для всех новых учетных записей пользователей пароли со случайным набором символов. Создание пароля со случайным набором символов будет способствовать обеспечению безопасности учетной записи пользователя.

Упражнение 2: изменение свойств учетной записи пользователя домена

В задании 1 упражнения 5 главы 6 Вы создали три учетные записи пользователей. Сейчас Вы будете работать с учетными записями Jane_Doe, John_Smith и Bob_Train с помощью оснастки Active Directory Users And Computers. Выполняйте упражнение на Server01.

► Задание 1: Измените параметры учетных записей пользователей

1. Зарегистрируйтесь на ServerOl как Administrator с паролем **password.**
2. Раскрыв меню Start\Programs\Administrative Tools, щелкните ярлык Active Directory Users And Computers.

   Откроется одноименная оснастка.
3. Раскройте в дереве консоли узел microsoft.com.
4. Выберите папку Users.
5. В правой панели дважды щелкните учетную запись Bob Train.

   Откроется диалоговое окно свойств учетной записи с выбранной вкладкой General (Общие). На вкладке General, помимо имени и фамилии, определяются и другие свойства учетной записи. Поиск пользователей облегчают поля Office (Комната) и Telephone Number (Номер телефона).
6. На вкладке Account (Учетная запись) щелкните кнопку Logon Hours (Время входа).

   Откроется диалоговое окно Logon Hours For Bob Train.

   Заметьте, что пользователю Bob вход в систему разрешен в любое время.
7. Чтобы ограничить время входа в систему пользователя Bob, щелкните время начала первого периода, в течение которого Вы хотите запретить ему вход в систему, и перетащите указатель на время окончания этого периода. Для этого определите текущие день и время и запретите вход на ближайшие 3 часа.

   Внимание! Чтобы данное ограничение работало правильно, выполните это упражнение в ближайшие три часа или увеличьте срок действия ограничения учетной записи на период, достаточный для завершения упражнения.

   Запретный период отображается в левой нижней части диалогового окна Logon Hours For Bob Train (Время входа для Bob Train).
8. Щелкните переключатель Logon Denied (Вход запрещен).

   Выделенный период изменит цвет на белый — пользователю запрещен вход в систему в течение этого срока.

   Совет Чтобы выбрать такой же период времени для всех дней недели, щелкните в поле All (Все) серый квадрат, представляющий начало периода, и перетащите указатель на время окончания. Чтобы выбрать день полностью, щелкните серый квадрат с его названием.

9. Чтобы закрыть диалоговое окно Logon Hours For Bob Train, щелкните кнопку OK.
10. Примените параметры, шелкнув OK в диалоговом окне Bob Train Properties.
11. На правой панели дважды щелкните John Smith.
    Откроется диалоговое окно свойств учетной записи John Smith с выбранной вкладкой General (Общие),
12. Перейдите на вкладку Account (Учетная запись).
13. Когда окончится срок действия данной учетной записи?
14. В группе Account expires (Срок действия учетной записи) щелкните переключатель End Of (Истекает) и задайте текущую дату.
15. Примените внесенные изменения, щелкнув кнопку OK.
16. Щелкните папку Sales в дереве консоли.
    В правой панели появится учетная запись Jane Doe.
17. Дважды щелкните учетную запись Jane Doe.
    Откроется окно Jane Doe Properties с выбранной вкладкой General.
18. Перейдите на вкладку Account.
19. В списке Account Options (Параметры учетной записи) пометьте флажок User Must Change Password At Next Logon (Потребовать смену пароля при следующем входе в систему).
20. Закройте окно Jane Doe Properties (Свойства: Jane Doe), щелкнув кнопку OK.
21. Закройте оснастку Active Directory Users And Computers.
22. В меню Start выберите команду Shut Down (Завершение работы).
    Откроется диалоговое окно Shut Down Windows (Завершение работы Windows).
23. Выбрав в списке Log OffAdministrator (Завершение сеанса Администратор), щелкните OK.
    Windows 2000 завершит сеанс пользователя Administrator и выведет на экран окно сообщения Welcome To Windows.
24. Нажмите клавиши Ctrl+Alt+Delete и перейдите к заданию 2.

► **Задание 2: попытайтесь войти на Server01 с учетной записью пользователя**

Вы используете для входа на Server0I учетную запись Jane Doe (Jane_Doe).

1. Войдите в систему без пароля как Jane_Doe.
   Появится сообщение, что срок действия Вашего пароля закончился и его следует сменить.
2. Щелкните кнопку OK.
   Откроется диалоговое окно Change Password с курсором в поле Old Password.
3. Поскольку учетной записи пользователя Jane_Doe не присвоен пароль, нажмите клавишу Tab.
4. В полях New Password и Confirm New Password, введите **student** и щелкните OK.
   Появится сообщение, что Ваш пароль изменился.
5. Закройте окно сообщения, щелкнув кнопку OK.
   Вошли ли Вы в систему? Почему?
6. Закройте окно сообщения, щелкнув кнопку OK.

► **Задание 3: предоставьте учетным записям пользователей права локального входа в систему**

Разрешить пользователям локальную регистрацию на контроллере домена можно по-разному. Вы добавите 3 пользователей, созданных в главе 6, к группе Print Operators (Операторы печати), имеющей право входить на контроллер домена.

Примечание Группа — это объединение учетных записей пользователей. Она облегчает администрирование, позволяя давать права всем ее членам, а не каждой индивидуальной учетной записи. Подробнее о группах — ниже в этой главе.

1. Зарегистрируйтесь в системе как Administrator с паролем password.
2. Откройте оснастку Active Directory Users And Computers и в дереве консоли раскройте ОП Sales.
3. В правой панели дважды щелкните учетную запись пользователя Jane Doe.
   Откроется диалоговое окно Jane Doe Properties (Свойства: Jane Doe) с выбранной вкладкой General.
4. Перейдите на вкладку Member Of (Член групп).
5. Щелкните кнопку Add (Добавить).
   Откроется диалоговое окно Select Groups (Выбор: Группа).
6. Щелкните Print Operators (Операторы печати).
7. Щелкните кнопку Add (Добавить), затем — OK, чтобы закрыть окно Select Groups (Выбор: Группа).
8. Закройте диалоговое окно Jane Doe Properties (Свойства: Jane Doe), щелкнув OK.
   Далее Вы используете более простой способ добавить учетные записи для Bob Train и John Smith в группу Print Operators.
9. Щелкните папку Users в дереве консоли.
10. В правой панели щелкните Bob Train и, удерживая клавишу Ctrl, щелкните John Smith.
11. В меню Action (Действие) выберите команду Add Members To Group (Добавить участников в группу).
    Откроется диалоговое окно Select Group.
12. Щелкните Print Operators (Операторы печати).
    Active Directory сообщит об успешном добавлении пользователей в группу.
13. Щелкните кнопку OK.
14. Закройте оснастку Active Directory Users And Computers и завершите свой сеанс.
15. Попытайтесь войти в систему как Jane_Doe с паролем student.
    Заметьте: Вы можете локально войти в систему по учетной записи Jane_Doe.
16. Попытайтесь войти в систему как Bob_Train без пароля.
    Вы не можете войти в систему из-за ограничения учетной записи пользователя. В задании 1 Вы ограничили время входа в систему пользователя Bob.
17. Попытайтесь войти в систему как John_Smith без пароля.
    Вам разрешен вход в систему по учетной записи John_Smith, В задании 1 Вы ограничили срок действия учетной записи этого пользователя до конца дня. Завтра войти в систему с его реквизитами будет нельзя,
18. Завершите свой сеанс на Server01.

Создание локальных учетных записей пользователей

Локальная учетная запись позволяет входить в систему и получать доступ к ресурсам только на том компьютере, на котором создана эта запись. Для создания локальных учетных записей служит оснастка Local Users And Groups (Локальные пользователи и компьютеры) (рис. 7-5).

Вы можете создать локальные учетные записи только на компьютерах с Windows 2000 Professional и изолированных или рядовых (не имеющих статуса контроллера) серверах

с Windows 2000 Server. Локальные учетные записи сохраняются не в каталоге домена, а в БД безопасности компьютера, на котором они были созданы.

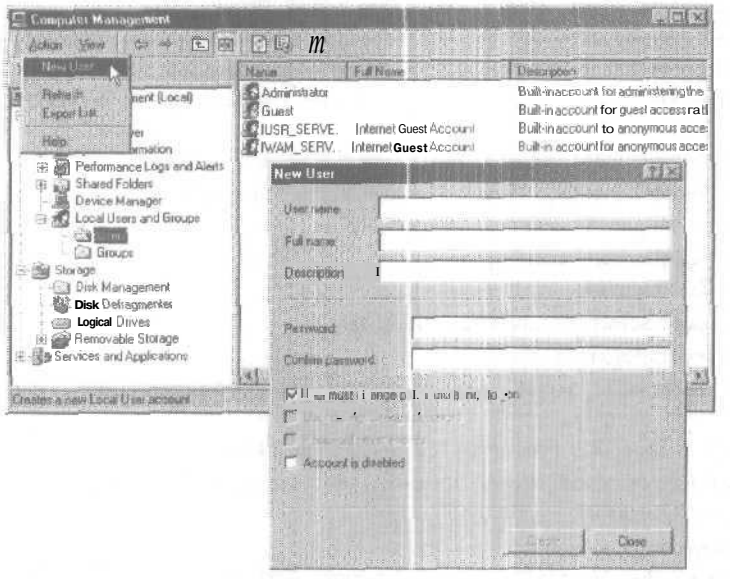


Рис. 7-5. Оснастка Local Users And Groups (Локальные пользователи и компьютеры) и диалоговое окно New User

Изменение свойств учетных записей пользователей

Набор свойств по умолчанию связан со всеми доменными и локальными учетными записями. Свойств у первых больше, чем у вторых. Свойства локальных учетных записей представляют собой подмножество свойств доменных учетных записей.

Свойства, определенные для доменных записей, применяются пользователями для поиска в хранилище Active Directory. Поэтому доменным учетным записям надо задавать подробные характеристики. Например, пользователь знает имя и телефон человека и хочет найти его фамилию. Фамилию можно найти по номеру телефона.

На основании потребностей конкретного пользователя для каждой доменной учетной записи необходимо настроить;

- личные реквизиты, включая информацию на вкладках General (Общие), Address (Адрес), Telephones (Телефоны) и Organization (Организация);
- параметры учетной записи;
- параметры времени входа;
- параметрырегистрации с рабочих станций.

Чтобы изменить доменную запись, в оснастке Active Directory Users And Computers дважды щелкните объект пользователя, свойства которого хотите изменить.

Чтобы изменить локальную учетную запись, в оснастке Computer Management, выберите Local Users And Groups (Локальные пользователи и группы) и дважды щелкните объект, свойства которого хотите изменить.

Диалоговое окно свойств

Содержит для всех учетных записей набор вкладок, позволяющих настраивать свойства для определенного пользователя. Вкладки General (Общие), Dial-In (Входящие звонки),

Member Of (Член групп) и Profile (Профиль) относятся к локальным учетным записям, остальные — к доменным.

Вкладки личных свойств

Включают вкладки General, Address, Telephones и Organization. Настройка атрибутов этих вкладок позволяет пользователям и администраторам искать пользователей в Active Directory:

Вкладка	Содержание
General (Общие)	Имя, местоположение офиса, телефон, адрес электронной почты и домашней страницы пользователя
Address (Адрес)	Улица, почтовый ящик, город, штат или провинция, почтовый индекс и страна проживания пользователя
Telephones (Телефоны)	Номера домашнего телефона, пейджера, мобильного телефона, факса, IP-телефона пользователя и комментарии
Organization (Организация)	Должность, отдел, руководитель и прямые подчиненные

Вкладка Account

Вкладка Account (Учетная запись) позволяет определять имя пользователя для входа в систему и задавать другие параметры учетной записи. Некоторые из этих параметров устанавливаются по умолчанию при создании объекта пользователя в хранилище Active Directory. Вы можете изменять эти свойства, а также настраивать дополнительные свойства.

Вкладка Profile

Профили пользователя автоматически создают и поддерживают индивидуальные параметры рабочего стола для работы пользователя на любом локальном компьютере домена. Вкладка Profile (Профиль) позволяет указать путь к сетевому ресурсу, где сохраняются профили пользователя. Кроме того, для учетной записи можно задать сценарий регистрации и домашнюю папку.

Вкладка **Published Certificates**

Сертификат (certificate) представляет собой набор данных для проверки подлинности и безопасного обмена информацией по незащищенным сетям, таким как Интернет. Сертификат гарантированно связывает открытый ключ шифрования с объектом, который содержит соответствующий закрытый ключ шифрования. Вкладка Published Certificates (Опубликованные сертификаты) отображает список сертификатов X.509 для учетной записи пользователя.

Вкладка Member Of

Группы применяются для упрощения администрирования. Например, предоставьте группе разрешение NTFS, а затем добавьте в нее нескольких пользователей. Полномочия распространяются на всех членов группы. Вкладка Member Of (Член групп) отображает группы, членом которых является пользователь.

Вкладка Dial-In

Вкладка Dial-In (Входящие звонки) позволяет контролировать, как пользователь выполняет телефонное подключение к сети. Для получения доступа к сети пользователь соединяется с компьютером, на котором работает служба Remote Access Service (RAS).

Примечание Помимо настройки параметров соединения и наличия службы RAS на сервере, к которому подсоединяется пользователь, надо настроить и коммутируемое соединение по телефону для сервера на компьютере клиента. Это поможет сделать мастер Network Connection (Мастер сетевого подключения), вызываемый из папки Network Connections (Сеть и удаленный доступ к сети) в Control Panel.

Параметры безопасного коммутируемого соединения таковы:

Параметр	Описание
Allow Access (Разрешить доступ)	Разрешает доступ по телефонной линии.
Deny Access (Запретить доступ)	Запрещает доступ по телефонной линии.
Verify Caller-ID (Проверять идентификатор)	Телефонный номер, с которого должен подсоединяться пользователь.
No Callback (Ответный вызов не выполняется)	Служба RAS сервера не будет делать ответный звонок пользователю, что позволяет ему звонить с любого телефона. Этот параметр задан по умолчанию для среды с низким уровнем безопасности или при применении других способов обеспечения безопасности телефонного соединения.
Set By Caller (Устанавливается вызывающим)	Пользователь предоставляет телефонный номер для ответного звонка службы RAS сервера, что позволяет ему позвонить с любого телефона, и служба RAS сервера сделает ему ответный звонок. Сведения о соединениях можно регистрировать в журнале. Применяется в среде со средним уровнем безопасности.
Always Callback To (Всегда по этому номеру)	Служба RAS сервера делает ответный звонок пользователю по указанному номеру. Пользователь должен находиться по заданному номеру для соединения с сервером, что снижает риск того, что соединение будет осуществлено неуполномоченным лицом, поскольку номер задан заранее. Применяется в среде с высоким уровнем безопасности.

Вкладка Object

На вкладке Object (Объект) отображается полное доменное имя объекта и дополнительные сведения, например, класс, даты создания и изменения объекта, исходный и текущий номера USN. Последние применяются для отслеживания изменений объектов в хранилище Active Directory.

Вкладка Security

Вкладка Security (Безопасность) позволяет установить разрешения для объекта пользователя в хранилище Active Directory. Вы можете настраивать специальные разрешения для групп и пользователей в пределах домена. Можно также задать дополнительные разрешения и указать параметры наследования разрешений от родительского объекта.

Вкладки служб терминалов

Вкладки Sessions (Сеансы), Environment (Среда), Remote Control (Удаленное управление) и Terminal Services Profile (Профиль служб терминалов) содержат сведения о пользователе служб Terminal Services: допустимое время входа в систему, параметры запускаемой программы и удаленного управления, а также профиль пользователя. Службы терминалов

позволяют пользователю входить в систему с компьютерного терминала и запускать на нем сеанс Windows 2000.

Вкладка Environment

Позволяет создать рабочую среду клиента. Если определена начальная программа, она автоматически запускается при каждом соединении пользователя с сервером терминалов. Это единственное приложение, с которым может работать пользователь. Закрытие этого приложения влечет обрыв соединения с сервером терминалов.

Учетную запись можно настроить и так, чтобы службы терминалов при входе в систему клиента автоматически подключали локальные диски и принтеры, При входе клиента на сервер определяются локальные диски и принтеры, и на сервере терминалов устанавливаются соответствующие драйверы принтера. Если установлено несколько принтеров, все задания печати можно по умолчанию перенаправлять на основной принтер клиента.

Вкладка Sessions

Здесь задаются параметры ограничения длительности сеансов на основе их текущего состояния (активны, бездействуют или отключены). Также можно определить действие, выполняемое по окончании времени сеанса.

Вот некоторые параметры вкладки Sessions:

Параметры тайм-аута	Описание
End A Disconnected Session (Завершение отключенного сеанса)	Задает максимальный срок активности на сервере отключенного сеанса, по истечении которого отключенный сеанс сбрасывается.
Active Session Limit . (Ограничения активного сеанса)	Задает максимальную продолжительность соединения. При истечении указанного времени сеанс либо отключается, оставаясь активным на сервере, либо сбрасывается.
Idle Session Limit (Ограничение бездействия сеанса)	Задает максимальную длительность простоя сеанса, после чего сеанс отключается или сбрасывается.

Вкладка Remote Control

Вкладка Remote Control (Удаленное управление) позволяет настроить свойства удаленного управления службами терминалов. Вы можете наблюдать за действиями клиента, вошедшего на сервер терминалов, из другого сеанса. Remote Control позволяет наблюдать или взаимодействовать с сеансом клиента. Выбрав последнее, Вы сможете при помощи клавиатуры и мыши воздействовать на сеанс клиента. Вы можете предупредить клиента, что желаете удаленно контролировать сеанс, выведя на экран сообщение клиенту с просьбой разрешить просмотр или участие в сеансе. Включить удаленный контроль учетной записи пользователя позволяют оснастка Local Users And Groups (для локальных пользователей) и Active Directory Users And Computers (для пользователей домена).

Примечание Этот параметр не разрешает удаленно управлять нетерминальными соединениями. Такие средства, как Systems Management Server (SMS), обеспечивают удаленное управление сетевыми компьютерами с ОС Windows.

Вкладка Terminal Services Profile

Вкладка Terminal Service Profile (Профиль служб терминалов) позволяет назначить пользователю профиль для терминального сеанса. Профиль служб терминалов применяется для ограничения доступа к приложениям путем их удаления из меню Start (Пуск) на компьютере пользователя. Администраторы также могут создавать и сохранять сетевые соединения с принтерами и другими ресурсами для применения во время пользовательских сеансов.

Вы можете задать путь к домашнему каталогу, используемому для терминальных сеансов. Этот каталог может быть или локальным, или общим сетевым ресурсом. Можно также определить, будет ли у пользователя доступ к службам терминалов. При отключенном параметре Allow Logon To Terminal Server (Разрешить вход на сервер терминалов) пользователю запрещено входить на любой сервер терминалов.

Администрирование учетных записей пользователей

Включает изменение учетных записей и настройку пользовательских профилей и домашних каталогов.

Профиль пользователя

Это набор папок и данных, определяющих параметры Вашего рабочего стола, приложений и место хранения личных данных. Профиль также содержит все сетевые соединения, установленные при входе в систему, пункты меню Start и драйверы, относящиеся к сетевым серверам. Профиль пользователя сохраняет вид рабочего стола и параметры среды, заданные во время последнего входа в систему.

Windows 2000 создает профиль локального пользователя при первом входе в систему. Профиль пользователя функционирует следующим образом.

- При входе в компьютер клиента с Windows 2000 Вы всегда получаете индивидуальные параметры рабочего стола и соединений независимо от того, кто ранее работал на этом компьютере.
- При первом входе Windows 2000 копирует папку Default User локального профиля в папку %systemdrive%\Documents and Settings\<*регистрационное_имя_пользователя*> (обычно это папка C:\Documents and Settings\<*регистрационное_имя_пользователя*>).
- Если компьютер, на котором Вы регистрируетесь, был обновлен с Windows 9x с включенными профилями или с Windows NT до Windows 2000 Professional, папкой профилей останется %systemroot%\profiles; она не будет создана в папке Documents And Settings.
- Папка профиля пользователя содержит много файлов и папок для хранения данных пользователя. Например, в папке My Documents хранятся личные файлы, она по умолчанию открывается при вызове в приложениях команд Open (Открыть) и Save As (Сохранить как). Windows 2000 по умолчанию создает ярлык My Documents на рабочем столе, что облегчает поиск личных документов.

Примечание Целевой каталог для папки My Documents можно изменить, открыв окно свойств ярлыка этой папки на рабочем столе.

- Самый простой способ изменить Ваш профиль пользователя — изменить параметры рабочего стола, например, при установке нового сетевого подключения или добавлении файла в папку My Documents. Затем при выходе из системы Windows 2000 вносит изменения в Ваш профиль. При следующем входе в систему появятся новое сетевое подключения и файл.

Примечание Рекомендуется, чтобы пользователи сохраняли свои документы в папке My Documents, а не в домашних каталогах. Windows 2000 автоматически устанавливает папку My Documents, и она по умолчанию является местом для сохранения данных приложениями Microsoft. Перенаправив папки и автономные папки (о них см. ниже), папку My Documents можно расположить в сети, и доступ к ней пользователи получат независимо от того, соединены они с сетью или нет,

---

Перемещаемый профиль пользователя

Для поддержки пользователей, работающих на нескольких компьютерах, настройте *перемещаемый профиль пользователя* (roaming user profile, RUP), установите его на сетевом сервере, чтобы он был доступен независимо от того, с какого компьютера они входят в домен. При входе в сеть Windows 2000 копирует такой профиль с сетевого сервера на компьютер, с которого входит пользователь. А значит, в любом месте сети он получает индивидуальные параметры рабочего стола и подключений.

При входе Windows 2000 применяет к данному компьютеру параметры RUP . При первом входе в систему на локальный компьютер копируются все документы пользователя. В дальнейшем при его входе Windows 2000 сравнивает локально сохраненные файлы профиля с файлами RUP. Система синхронизирует их, копируя только те файлы, что изменялись со времени последнего входа пользователя в систему. Поскольку Windows 2000 копирует только их, вход в систему ускоряется.

При выходе пользователя из системы Windows 2000 копирует сделанные в локальной копии RUP изменения обратно на сервер.

Настройка перемещаемого профиля

Можно настроить или указать готовый RUP для всех учетных записей и запретить его модификацию. Для этого можно настроить рабочую среду и скопировать полученный профиль на место RUP пользователя.

Перемещаемые профили используются для:

- обеспечения пользователей рабочей средой, включающей только необходимые для работы подключения и приложения;
- обеспечения стандартной среды рабочего стола для RUP пользователей, имеющих одинаковые требования к работе; им нужны одинаковые сетевые ресурсы;
- устранения ошибок: имея ясное представление о настройке рабочих столов пользователей, специалисты службы технической поддержки найдут отклонение или проблему.

Примечание Вы можете настраивать локальные профили, но это не рекомендуется. Они располагаются только на компьютере клиента, с которого он входит в сеть. Так что Вам придется создавать локальный профиль на каждом компьютере, с которого регистрируется клиент.

Обязательный профиль

Так называют RUP «только для чтения». Пользователь по-прежнему может изменять параметры своего рабочего стола, но при выходе из системы эти изменения не сохраняются. При его следующем входе обязательный профиль снова загружается с сервера.

Вы можете назначить один обязательный профиль многим пользователям, которым нужны одинаковые параметры рабочего стола. Изменив один профиль, Вы измените рабочую среду нескольких пользователей.

Чтобы сделать профиль обязательным, переименуйте файл Ntuser.dat, расположенный на сервере, в Ntuser.man. Файл профиля с этим расширением будет доступен только для чтения.

Настройка перемещаемого профиля пользователя

Если настроить на сервере RUP, при следующем входе пользователя на компьютер в домене Windows 2000 скопирует локальный профиль пользователя в папку RUP на сервер. При следующем входе пользователя в систему RUP будет скопирован с сервера на компьютер пользователя.

Храните перемещаемые профили на часто архивируемом сервере. Для ускорения входа в систему в сильно загруженной сети поместите папки RUP на рядовой сервер, а не на контроллер домена. Копирование RUP с сервера на компьютеры клиентов может занять значительную часть полосы пропускания сети и усилить нагрузку на процессоры компьютеров. Хранение профилей на контроллере домена замедляет проверку подлинности (аутентификацию) пользователей в домене.

Совет Для повышения производительности и доступности профилей настройте доменный корень DFS для профилей пользователей и сконфигурируйте FRS, чтобы профили копировались в несколько мест в сети.

Чтобы настроить RUP, надо создать общую папку на сервере и задать путь в формате \\<*сервер*>\<*ресурс*> Используйте интуитивное имя для общей папки, например, Profiles. На вкладке Profile (Профиль) в диалоговом окне свойств учетной записи назначьте путь к общей папке в поле Profile Path (Путь к профилю) — \\<*сервер*>\<*ресурс*>\<*регистрационное_имя*>.

Вместо регистрационного имени можно указать переменную %username% — Windows 2000 автоматически заменяет ее именем учетной записи пользователя.

Назначение перемещаемого профиля пользователя

Можно настроить RUP и назначить его нескольким пользователям — вследствие этого при входе в систему у них будут одинаковые параметры и подключения. До создания и назначения RUP надо создать шаблон профиля, включающий параметры рабочего стола, которые, по Вашему мнению, должны быть у пользователей. Шаблон создается путем придания рабочему столу точно такого вида, какой должен быть у пользователей, которым назначен данный профиль. Создание данного шаблона не требует специальных средств.

Создав шаблон профиля пользователя, войдите в систему как Administrator и скопируйте шаблон в папку перемещаемого профиля на сервере. Папка должна быть доступна для всех пользователей, которым будет назначен этот профиль. Шаблон профиля копируется на общий сетевой ресурс с помощью приложения System (Система) из Control Panel (рис. 7-6; профиль назначен встроенной группе Users в домене).

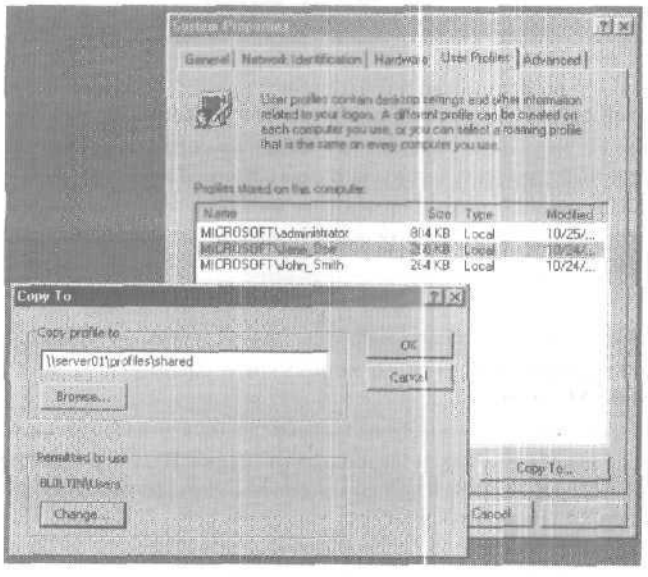


Рис. 7-6. Копирование шаблона профиля Jane_Doe в общий подкаталог \\server01\profiles

Чтобы завершить данный процесс, при помощи оснастки Active Directory Users And Computers назначьте профиль соответствующему пользователю. Открыв оснастку, в окне свойств учетной записи перейдите на вкладку Profile и задайте путь к профилю в поле Profile path (Путь к профилю).

Поскольку изменения в шаблоне профиля касаются всех пользователей, которым назначен этот профиль, его надо сделать обязательным. Чтобы сделать профиль обязательным («только для чтения»), измените расширение файла Ntuser в каталоге профиля на сервере с .dat на .man.

Примечание Файл Ntuser.dat является скрытым. Снять атрибут «скрытый» поможет утилита командной строки attrib, или измените свойства этого файла, включив просмотр скрытых файлов в Windows Explorer.

Изменение учетных записей пользователей

Интересы предприятия могут потребовать изменения учетных записей, скажем, переименовать учетную запись для нового сотрудника так, чтобы он имел полномочия и доступ к сети своего предшественника. Другие изменения — например, отключение, подключение или удаление учетной записи — касаются персональных изменений или личной информации. Может потребоваться и восстановление пароля или разблокирование учетной записи.

Примечание Учетная запись изменяется путем изменения объекта учетной записи пользователя в хранилище Active Directory. Для успешного изменения учетных записей, создания RUP и назначения домашних каталогов надо иметь право на администрирование ОП, к которому относятся учетные записи.

Отключение, включение, переименование и удаление учетных записей пользователей

Вы можете производить следующие действия.

- Отключение/включение. Учетную запись следует отключать, когда пользователю в течение длительного времени она будет не нужна, но понадобится в будущем. Например, если Алексей уходит в отпуск, отключите его учетную запись, а когда он вернется, Вы ее включите.
- Переименование. Учетные записи переименовываются, когда надо сохранить все права, разрешения, членство в группе и большинство других свойств одной учетной записи и переназначить их другой. Например, если в организации появился новый бухгалтер, переименуйте учетную запись, изменив имя, фамилию и пароль пользователя для нового бухгалтера.
- **Удаление.** Удаляйте учетные записи уволенных сотрудников (если Вы не собираетесь их переименовывать).

Процедуры отключения, включения, переименования и удаления доменных и локальных учетных записей похожи. Для доменных учетных записей используйте оснастку Active Directory Users And Computers. Выберите учетную запись и щелкните в меню Action соответствующую команду. Для локальных учетных записей используйте расширение Local Users And Groups оснастки Computer Management.

Примечание Если учетная запись пользователя включена, в меню Action Вы увидите команду Disable Account (Отключить учетную запись). Если учетная запись отключена, в меню Action появится команда Enable Account (Включить учетную запись).

Восстановление паролей и разблокирование учетных записей пользователей

Если пользователь не может зарегистрироваться в домене или на локальном компьютере, может потребоваться смена его пароля или разблокирование его учетной записи. Для этого Вам надо иметь административные привилегии для ОП, к которому относится данная учетная запись.

Смена паролей

Если срок действия пароля истечет до того, как его изменят, или пользователь забудет свой пароль, Вам надо сменить пароль.

Примечание Для этого старый пароль знать не обязательно.

Откройте оснастку Active Directory Users And Computers и выберите объект пользователя. В меню Action выберите команду Reset Password (Смена пароля). В диалоговом окне Reset Password введите пароль и помгтьте флажок User Must Change Password At Next Logon (Потребовать смену пароля при следующем входе в систему).

Разблокирование учетных записей пользователей

Групповая политика Windows 2000 блокирует учетную запись пользователя, нарушившего политику, например, превысившего допустимое число неудачных попыток входа в систему, Если учетная запись заблокирована, Windows 2000 сообщает об ошибке. Чтобы разблокировать учетную запись, в оснастке Active Directory Users And Computers щелкните правой кнопкой объект пользователя, выберите в контекстном меню команду Properties (Свойства) и на вкладке Account (Учетная запись) сбросьте флажок The Account Is Locked Out (Заблокировать учетную запись).

Создание домашней папки

Помимо папки My Documents, Windows 2000 позволяет создать дополнительную — домашнюю — папку пользователя, которую Вы можете выделить ему для хранения личных документов и старых приложений. Иногда она является папкой по умолчанию для сохранения документов. Вы можете хранить домашнюю папку на компьютере клиента или в общей папке на файловом сервере. Домашняя папка не является частью RUP, поэтому ее размер не влияет на сетевой трафик при входе в систему. Вы можете разместить все домашние папки централизованно на сетевом сервере. Хранение всех домашних папок на файловом сервере дает ряд преимуществ:

- пользователи могут получать доступ к своим домашним папкам с любого компьютера в сети;
- централизованная поддержка и администрирование документов пользователя;
- домашние папки доступны с компьютера клиента, на котором работает любая ОС Microsoft (включая MS-DOS, Windows 9x/2000).

Примечание Храните домашние папки на томе NTFS, чтобы можно было задействовать разрешения NTFS для защиты документов пользователей. Если домашние папки хранятся на томе FAT, можно ограничить доступ к ним только посредством разрешений доступа к общим папкам.

Для создания домашней папки на файловом сервере в сети выполните следующее.

- Создание и открытие доступа к папке. Создайте и откройте совместный доступ к папке, в которой будут храниться все домашние папки на сетевом сервере. Домашняя папка для всех пользователей будет вложена в эту общую папку.

- **Изменение разрешения Full Control.** Для общей папки удалите разрешение по умолчанию Full Control (Полный доступ) для группы Everyone (Все) и назначьте его группе Users (Пользователи). Это гарантирует, что доступ к общей папке получат только пользователи с доменными учетными записями.
- **Укажите путь к домашней папке.** Укажите путь на вкладке Profile (Профиль) диалогового окна свойств учетной записи в группе Home folder (Домашняя папка) (рис. 7-7). Поскольку домашняя папка находится на сетевом сервере, щелкните Connect (Подключить) и укажите букву подключаемого диска. Тогда при подключении пользователя к сети определенное Вами имя диска появится в окне My Computer, В поле To (к) появится имя UNC в виде *<сервер>**<ресурс>**<регистрационное_имя_пользователя>*. В качестве имени пользователя укажите переменную %username%, чтобы автоматически присвоить имя и создать домашнюю папку пользователя с тем же именем, под каким он входит в систему.

Примечание Если Вы задаете имя папки на томе NTFS с помощью переменной %username%, пользователь и участники встроенной локальной группы Administrators получат для нее разрешение Full Control. Все другие разрешения для этой папки удаляются, включая права группы Everyone.

Вы можете расширить свойства домашней папки, перенаправив пользователя от папки My Documents к месту расположения его домашнего каталога.

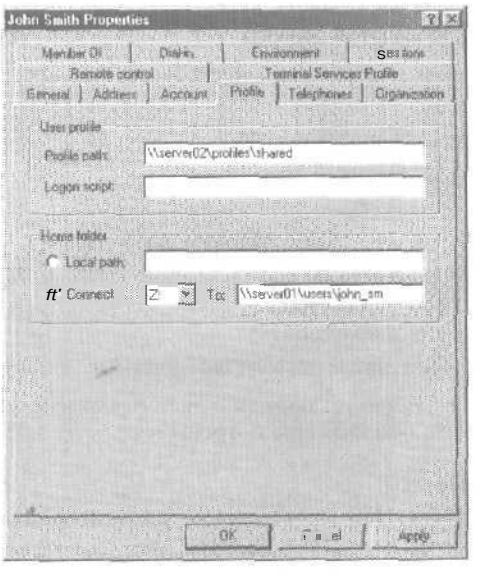


Рис. 7-7. Вкладка Profile (Профиль) в окне свойств учетной записи пользователя; заданы путь к профилю и путь к общей сетевой домашней папке

Упражнение 3: создание RUP и назначение домашней папки

Вы создадите профиль, применив учетную запись Jane_Doe. Затем, чтобы создать локальный профиль для учетной записи, Вы войдете в систему как Jane Doe. Затем Вы войдете в систему как Administrator и с помощью приложения System (Система) в Control Panel убедитесь, что нужный профиль создан. В задании 2 с по-

мощью этого профиля Вы создадите и проверите RUP со второго компьютера. В задании 3 Вы создадите и проверите домашнюю папку для Jane_Doe.

► Задание 1: создайте шаблон профиля пользователя

Вы определите и проверите локальный профиль пользователя. На Server01 Вы создадите шаблон профиля пользователя. Обычно для создания шаблона применяется компьютер с Windows 2000 Professional, но здесь предполагается, что задания выполняются на Windows 2000 Server.

1. Если Вы зарегистрированы на Server01как Administrator, завершите сеанс.
2. Войдите в домен microsoft.com как Jane_Doe с паролем student.

   Если при этом Вы использовали учетную запись Jane_Doe первый раз, создается стандартный локальный профиль. Он будет перенастроен и назначен другим пользователям.
3. Дважды щелкните значок My Computer на рабочем столе.

   Откроется одноименное окно.
4. Перетащите значок Local Disk (C:) [Локальный диск (C:)] на рабочий стол.

   Вы увидите сообщение о том, что данный элемент не может быть скопирован или перемещен, но для него можно создать ярлык.
5. Щелкните кнопку Yes (Да) для создания ярлыка для диска C:.
6. Закройте окно My Computer (Мой компьютер).
7. Раскройте меню Start\Settings (Пуск\Настройка) и щелкните ярлык Control Panel. В открывшемся окне дважды щелкните значок Display (Экран).

   Откроется диалоговое окно Display Properties (Свойства: Экран).
8. Перейдите на вкладку Appearance (Оформление).

   Обратите внимание на текущую цветовую схему.
9. В списке Scheme (Схема) выберите другую схему и щелкните OK.

   Рабочий стол изменится в соответствии с новой цветовой схемой.
10. Закройте окно Control Panel.
11. Завершив сеанс Jane_Doe, войдите снова как Administrator с паролем password.
12. Раскрыв меню Start\Settings (Пуск\Настройка), щелкните ярлык Control Panel. В открывшемся окне дважды щелкните значок System (Система).
13. Перейдите на вкладку User Profiles (Профили пользователей).

    Заметьте: на ServerOl несколько профилей. Они представляют все учетные записи пользователей на Server01.
14. Не закрывайте приложение System (Система) — оно Вам еще потребуется.

► Задание 2: определите и назначьте обязательный RUP

Из профиля пользователя Jane_Doe Вы создадите RUP и назначите его учетной записи John Smith. Выполняйте все действия на Server01. Чтобы проверить RUP, можете войти в систему с Server02.

Примечание Этот этап предполагает, что Вы знаете, как создать папку и открыть к ней доступ (см. занятие 1 главы 5).

---

1. Создайте на диске C:\ папку с именем Profiles.
2. Создайте обший ресурс с именем Profiles для палки C:\Profiles.
3. Откройте папку Profiles и создайте подпапку Shared.

   Закройте окно Profiles.

4. Найдите диалоговое окно System Properties (Свойства системы). Приложение System было открыто на предыдущем задании.
5. Перейдите на вкладку User Profiles (Профили пользователей).
6. В списке Profiles Stored On This Computer (Профили, хранящиеся на этом компьютере) выберите MICROSOFT\Jane_Doe.
7. Щелкните кнопку Copy To (Копировать).

   Откроется диалоговое окно Copy To (Копирование профиля).
8. В поле Copy Profile to (Копировать профиль на) наберите **\\server01\profiles\shared**.
9. Щелкните кнопку Change (Изменить).

   Откроется диалоговое окно Select User Or Group (Выбор: Пользователь или Группа).
10. В столбце Name (Имя) щелкните Users (Пользователи) и затем — кнопку OK.

    В группе Permitted To Use (Разрешить использование) появится надпись BUILTIN\Users.
11. Щелкните кнопку OK для возврата в окно System Properties.

    Вы увидите сообщение, что папка \\server01\profiles\shared уже существует и текущее содержимое будет удалено. Такое сообщение появилось потому, что папку для этого профиля Вы уже создали.
12. Щелкните кнопку Yes (Да).
13. Щелкните кнопку OK для возврата в окно Control Panel.
14. Откройте оснастку Active Directory Users And Computers.
15. Раскройте узел microsoft.com и щелкните папку Users.
16. В правой панели дважды щелкните учетную запись пользователя John Smith.

    Откроется диалоговое окно ее свойств.
17. Ранее Вы установили срок действия учетной записи этого пользователя. Чтобы удалить этот срок действия, на вкладке Account (Учетная запись) щелкните переключатель Never в группе Account Expires (Срок действия учетной записи).
18. Перейдите на вкладку Profile.
19. В поле Profile path (Путь к профилю) наберите **\\server01\profiles\shared** и щелкните OK.

    Закройте оснастку Active Directory Users And Computers.

    Так как Вы используете централизованный профиль, который должен быть назначен другим пользователям, сделайте его обязательным.
20. Дважды щелкните значок My Computer (Мой компьютер) на рабочем столе.
21. Дважды щелкните значок Local Disk (C:) [Локальный диск (C:)].
22. Дважды щелкните папку Profiles.
23. Дважды щелкните папку Shared.

    Заметьте, что открылись папки профиля.
24. В меню Tools (Сервис) выберите команду Folder Options (Свойства папки).

    Откроется одноименное диалоговое окно.
25. Перейдите на вкладку View (Вид).
26. Щелкните переключатель Select the Show Hidden Files And Folders (Показывать скрытые файлы и папки) и сбросьте флажок Hide File Extensions For Known File Types (Скрывать расширения для зарегистрированных типов файлов).
27. Щелкните кнопку OK.

    Откроется окно Shared, показывающее скрытые файлы и папки, включая файл Ntuser.dat.
28. Выберите файл Ntuser.dat.
29. В меню File (Файл) выберите команду Rename (Переименовать).
30. Измените расширение файла на .man и нажмите клавишу Enter.
31. Закройте окно Shared и окно Control Panel (Панель управления).

32. Завершите текущий сеанс и войдите в систему как John_Smith без пароля.

    Откроется рабочий стол пользователя John_Smith. Убедитесь, что его цветовая палитра именно та, что Вы назначили шаблону профиля пользователя и что на рабочем столе появился ярлык диска C:.

33. Для проверки обязательного профиля удалите с рабочего стола ярлык Connect To The Internet (Подключение к Интернету).
34. Завершите текущий сеанс и войдите в систему как John_Smith без пароля.

    На рабочем столе появился ярлык Connect to the Internet. Это произошло потому, что Вы назначили учетной записи John_Smith обязательный профиль.

► Задание *3:* назначьте **пользователю домашнюю** папку

На этом этапе Вы назначите John_Smith домашнюю папку.

1. Завершите сеанс John_Smith и войдите как Administrator с паролем password.
2. Создайте на диске C: папку HomeDirs.
3. Сделайте папку HomeDirs общей.
4. Откройте оснастку Active Directory User And Computers.
5. Открыв окно свойств учетной записи John_Smith, перейдите на вкладку Profile.
6. В разделе Home Folder (Домашняя папка) щелкните переключатель Connect (Подключить),
7. **Проверьте, что справа от переключателя Connect в списке** появился **диск** Z:.
8. В поле To (к) наберите **\\server01\HomeDirs\%username%** и щелкните кнопку OK.
9. Закройте оснастку Active Directory Users And Computers.
10. Щелкните папку HomeDirs в Windows Explorer (Проводник).
11. В меню File (Файл) выберите команду Properties (Свойства).

    Откроется диалоговое окно свойств папки HomeDirs.

12. Перейдите на вкладку Security (Безопасность).

    Заметьте, что группа Everyone (Все) имеет разрешение Full Control (Полный доступ) для этого каталога.

13. Щелкните кнопку Add (Добавить).

    Откроется диалоговое окно Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или Группы).

14. **Выберите Users (Пользователи)** и щелкните **кнопку Add** (Добавить).
15. Щелкните кнопку OK.

    Откроется диалоговое окно свойств палки HomeDirs, показывающее группы Everyone (Все) и MICROSOFT\Users. Убедитесь, что группе Users назначены права Read & Execute (Чтение и выполнение); List Folder Contents (Список содержимого папки) и Read (Чтение).

16. Сбросьте флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект).

    Появится сообщение Security (Безопасность).

17. Прочитайте сообщение и щелкните кнопку Remove (Удалить).

    Группа Everyone (Все) больше не имеет прав доступа к папке HomeDirs.

18. Щелкните кнопку Add (Добавить).

    Откроется диалоговое окно Select Users, Computers, Or Groups.

19. Выберите группу Administrators и щелкните кнопку Add.
20. Щелкните кнопку OK.

    Откроется диалоговое окно свойств папки HomeDirs, показывающее группы MICROSOFT\Users и MICROSOFT\Administrators.

21. Выберите группу Administrators (Администраторы).
22. В списке Permissions (Разрешения) пометьте флажок Allow (Разрешить) в строке Full Control (Полный доступ).

    Все флажки должны быть помечены.
23. Щелкните кнопку OK.
24. Дважды щелкните папку HomeDirs.
25. Щелкните папку John_Smith.
26. В меню File (Файл) выберите команду Properties (Свойства).

    Откроется диалоговое окно John Smith Properties.
27. Перейдите на вкладку Security (Безопасность).

    Заметьте, что Administrators и John Smith получили полный контроль над этим каталогом. Эти произошло автоматически, когда Вы задали как домашнюю папкой для учетной записи John_Smith папку \\server01\HomeDirs\%username%.
28. Щелкните кнопку OK и закройте Windows Explorer (Проводник).
29. Завершите сеанс Administrator и войдите снова как John_Smith без пароля.
30. Дважды щелкните значок My Computer (Мой компьютер).

    Заметьте: появился новый значок сетевого диска Z:, указывающий на подпапку John_Smith папки \\server01\HomeDirs.
31. Закройте окно My Computer и выйдите из системы.

Резюме

Учетная запись позволяет пользователю регистрироваться в домене для доступа к сетевым ресурсам или на локальном компьютере для доступа к ресурсам этого компьютера. Windows 2000 предусматривает доменные и локальные учетные записи. Встроенные учетные записи пользователей применяются для администрирования или для доступа к сетевым ресурсам. Прежде чем начать создавать учетные записи, надо спланировать правила их наименования, требования к паролям и параметры учетных записей, например, время входа в систему. Доменная учетная запись создается в оснастке Active Directory Users And Computers, а локальная — в оснастке Local Users And Groups. Все доменные и локальные учетные записи имеют стандартный набор свойств. Эти свойства можно изменять в диалоговом окне свойств. Администрирование учетных записей включает их изменение, а также управление профилями пользователей и домашними папками. Профиль пользователя — это набор папок и данных, определяющий рабочую среду пользователя. Для хранения личных документов и старых приложений можно предоставить пользователям домашнюю папку; иногда она является папкой по умолчанию для сохранения документов.

Занятие 3. Администрирование учетных записей групп

Мы рассмотрим группы и их реализацию в среде Windows 2000. Вы узнаете, что такое группы и как они упрощают администрирование учетных записей пользователей, Кроме того, мы обсудим типы групп и реализацию групп в домене, а также реализацию локальных и встроенных групп.

Изучив материал этого занятия, Вы сможете:

- ✓ **реализовать** группы **в домене;**
- ✓ реализовать локальные и встроенные группы.

Продолжительность занятия — около 60 минут.

Группы

Группа (group) — это набор учетных записей пользователей. Группы упрощают администрирование, позволяя назначать разрешения и права группе пользователей, а не каждой отдельной учетной записи. Пользователи могут быть членами нескольких групп.

Назначая разрешения, Вы предоставляете пользователям доступ к определенным ресурсам и определяете права доступа. Если, например, нескольким пользователям требуется считать один файл, добавьте их учетные записи в группу. Затем дайте группе разрешение на считывание файла. Права дают возможность выполнять системные задачи, например изменять системное время, архивировать или восстанавливать файлы, а также локально регистрироваться в системе.

Кроме пользователей, в группу можно добавлять контакты, компьютеры и другие группы. Добавляя компьютеры в группу. Вы можете упростить предоставление доступа системной задаче одного компьютера к ресурсам другого.

Реализация групп в домене

Для внедрения групп в домене надо понимать типы групп, области действия групп и правила членства в группе. Эти знания помогут Вам создавать группы, добавлять в них новых участников, изменять область действия группы и удалять их.

Примечание В документации по Windows 2000 доменные группы называются просто группами, а остальные — локальными или встроенными. Подробнее об упомянутых типах групп см. далее в этом занятии. Вместе с тем термин *группа* часто используется в общем смысле и относится к любому типу групп, который можно реализовать в Windows 2000.

Типы групп

Иногда группы создаются в целях защиты, например, для назначения разрешений. В других случаях создание групп не связано с соображениями безопасности, и они используются, например, для отсылки сообщений электронной почты. Таким образом, в Windows 2000 Server два типа групп: безопасности и распространения. Тип группы определяет порядок ее использования. Группы обоих типов размешаются в хранилище Active Directory, что позволяет их применять в любом сегменте сети.

Группы безопасности

В ОС Windows 2000 доступны только группы безопасности, используемые для назначения разрешений и предоставления доступа к ресурсам. Программы поиска в хранилище Active Directory также могут использовать группы безопасности в целях, не связанных с безопасностью, например, для одновременной отсылки сообщений электронной почты нескольким пользователям. Следовательно, группа безопасности обладает всеми возможностями группы распространения.

Группы распространения

Приложения используют группы распространения в качестве списков пользователей для осуществления функций, не связанных с системой защиты. Группы распространения следует применять лишь для выполнения операций, не связанных с безопасностью, например для одновременной отсылки сообщений электронной почты нескольким пользователям. Назначать разрешения через группу распространения нельзя.

Примечание Группы распространения могут использоваться лишь приложениями, предназначенными для работы со службой каталогов Active Directory. Например, будущие версии Microsoft Exchange Server смогут обращаться к группам распространения как к спискам распространения для рассылки электронной почты.

Область действия группы

При создании группы надо определить ее тип и область действия (рис. 7-8), которая позволяет по-разному использовать группы для назначения разрешений.

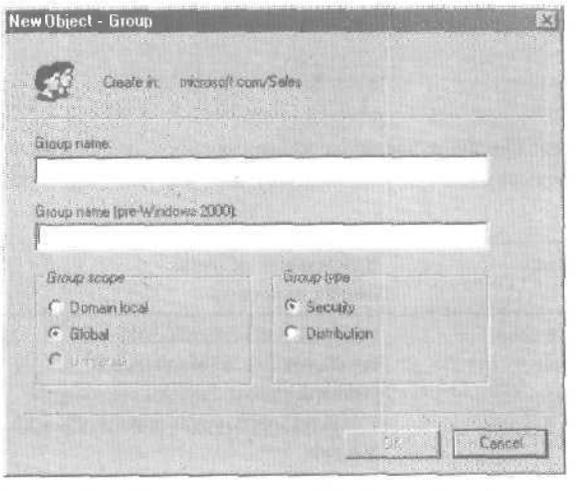


Рис. 7-8. **Диалоговое окно** New **Object — Group (Новый объект — группа), открытое в оснастке Active Directory Users** And **Computers (Active** Directory **— пользователи и компьютеры) для ОП Sales**

Область действия также определяет, в каких сегментах сети группу можно использовать. По области действия группы делятся на локальные группы домена, глобальные и универсальные.

Локальная группа домена

Чаще всего используется для назначения разрешений доступа к ресурсам. Ее характеристики:

- **открытое членство** — можно добавлять членов из любого домена;
- **доступ к ресурсам одного домена** — позволяет назначать разрешения доступа к ресурсам того же домена, где была создана группа.

Глобальная группа

Чаще всего применяется для организации пользователей с одинаковыми требованиями доступа к сети. Ее характеристики;

- **ограниченное членство** — можно добавлять членов лишь из того домена, где создана группа;
- **доступ к ресурсам любого** домена — позволяет назначать разрешения доступа к ресурсам любого домена.

Универсальная группа

Чаще всего применяется для назначения разрешений доступа к связанным ресурсам, находящимся в нескольких доменах. Ее характеристики:

- **открытое членство** — можно добавлять участников из любого домена;
- доступ **к ресурсам любого** домена — позволяет назначать разрешения доступа к ресурсам в любом домене;
- **доступна лишь в доменах основного режима** — в доменах смешанного режима эти группы недоступны; полный набор возможностей Windows 2000 доступен лишь в основном режиме; на рис. 7-8 универсальная группа недоступна, так как сервер работает в смешанном режиме и в области Group Type (Тип группы) выбран переключатель Security (Группа безопасности); универсальные группы распространения доступны в смешанном режиме.

Участники групп

Обусловлены областью действия группы. Правила членства устанавливают, кого можно включить в группу. К членам групп относятся учетные записи пользователей и другие группы. Правила членства таковы:

Группа по области действия	**В смешанном** режиме **может включать**	**В основном режиме может включать**
Локальная группа домена	Учетные записи пользователей и компьютеров, а также глобальные группы из любого домена	Учетные записи пользователей, компьютеров, глобальные и универсальные группы, входящие в любую локальную группу того же домена
Глобальная группа	Учетные записи пользователей из того же домена и учетные записи компьютеров	Учетные записи пользователей и компьютеров, а также глобальные группы из того же домена
Универсальная группа	В смешанном режиме недоступна	Учетные записи пользователей и компьютеров, глобальные и универсальные группы из любого домена

Локальные доменные и глобальные группы можно преобразовать в универсальные. Для этого надо, чтобы хранилище Active Directory работало в основном режиме, локальные доменные/глобальные группы не содержали Других участников из той же области действия. Например, глобальную группу, включающую другую глобальную группу, преобразовать в универсальную нельзя.

Примечание На группы распространения, работающие в смешанном режиме, распространяются те же правила членства, что и на группы защиты, работающие в основном режиме.

Вложенность групп

Добавление одних групп в другие (вложенность трупп) позволяет на порядок снизить число операций по назначению разрешений. Изучите потребности членов групп и создайте соответствующую иерархию групп. В основном режиме Windows 2000 допускает неограниченную вложенность групп.

Так, можно создать группу для каждого региона, в котором имеются филиалы организации, затем добавить менеджеров из всех регионов в отдельные группы. Все региональные группы можно добавить в группу Worldwide Managers. Если региональным менеджерам потребуется доступ к некоторому ресурсу, задайте соответствующие разрешения группе Worldwide Managers. Благодаря вложенности, эта группа включает всех членов региональных групп, поэтому менеджеры из всех регионов смогут обратиться к требуемому ресурсу. Это обеспечивает упрощенное иерархичное назначение разрешений, а также децентрализованный контроль членства.

При добавлении одних групп в другие попытайтесь снизить уровень вложенности. Вложенность позволяет на порядок снизить число операций по назначению разрешений. Однако при больших уровнях вложенности контроль разрешений усложняется. Наиболее эффективен первый уровень — он позволяет снизить число операций по назначению разрешений, одновременно упрощая контроль разрешений.

Кроме того, в целях контроля за назначением разрешений рекомендуется отдельно документировать состав групп. Допустим, администратор добавляет временных сотрудников в группу, созданную для разработчиков некоторого проекта. Другой администратор, не зная о временных сотрудниках, добавляет труппу проекта в труппу, обладающую доступом к конфиденциальной информации, и временные сотрудники получают к ней доступ, что неприемлемо.

Эффективная вложенность групп в многодоменной среде позволит снизить сетевой трафик между доменами и упростить администрирование дерева доменов. Для эффективного использования вложенности надо понимать правила членства в группах.

Вы должны учитывать, какие группы создают меньший трафик междоменной репликации. Например, Windows 2000 реплицирует только глобальную группу; список ее членов не тиражируется. Надо учитывать и режим работы дерева домена:

- в смешанном режиме доступен лишь один вид вложенности — глобальные группы любого домена могут входить в локальные группы доменов; в смешанном режиме универсальные группы недоступны;
- в основном режиме доступны все правила членства в группах, допускаются множественные уровни вложенности.

Стратегии групп

Для эффективной работы надо определить порядок использования групп, а также типы групп, которые будут задействованы в конкретных ситуациях.

Использование глобальных и локальных групп домена

Правила реализации глобальных и локальных групп домена идентичны рекомендациям по созданию стратегий групп для доменов Windows **NT** 3.x/4.0. Надо:

- пользователей со схожими обязанностями объединить в одну группу; например, в бухгалтерии можно объединить учетные записи бухгалтеров в группу Accounting;
- определить, к каким ресурсам или группам ресурсов обращаются сотрудники, и создать для этого ресурса локальную группу домена; например, если в организации несколько цветных принтеров, создайте локальную группу домена Color Printers;
- выявить все глобальные группы, обращающиеся к одним и тем же ресурсам, и включить эти группы в соответствующую локальную группу домена; так. можно добавить глобальные группы Accounting, Sales и Management в локальную группу домена Color Printers;
- назначить локальной группе домена соответствующие разрешения; например, группе Color Printers надо назначить разрешения на доступ к цветным принтерам.

Стратегия глобальных и локальных групп домена представлена на рис. 7-9. Поместите учетные записи пользователей в глобальные группы, создайте для совместно используемых ресурсов локальную группу доме на, включите глобальные группы в локальную и предоставьте локальной группе домена нужные разрешения.

Кроме того, помещая учетные записи пользователей в локальные группы домена и назначая последним разрешения, Вы не можете предоставлять разрешения вне домена. Гибкость стратегии глобальных и локальных групп домена снижается с ростом сети.

Несмотря на преимущества данной стратегии, при работе с несколькими доменами размещение учетных записей в глобальных группах и назначение им разрешений может усложнить администрирование. Если глобальным группам нескольких доменов нужны одинаковые разрешения, придется назначать их каждой группе в отдельности.

Рис. 7-9. Планирование стратегии групп

Использование универсальных групп

Универсальные группы — одна из новых возможностей Windows 2000.

- Используйте их для предоставления доступа к ресурсам нескольких доменов. В отличие от локальных доменных, универсальным группам можно назначать разрешения на доступ к ресурсам любого домена Вашей сети. Например, если ответственным лицам требуется доступ ко всем принтерам сети, можно создать универсальную группу и назначить ей разрешения на использование принтеров, подключенных к серверам печати всех доменов.
- Их рекомендуется использовать, только если их состав постоянен. При изменении состава универсальной группы в дереве доменов может возникнуть ненужный трафик между контроллерами доменов, поскольку такие изменения реплицируются на многие контроллеры доменов.
- Рекомендуется, объединив глобальные группы нескольких доменов в универсальную группу, присвоить ей разрешения на доступ к ресурсу. Таким образом, универсальную группу можно использовать аналогично локальным группам домена для назначения разрешений доступа к ресурсам. И все же, в отличие от локальной доменной, универсальной группе можно назначать разрешения доступа к ресурсам других доменов.

Внедрение групп

Разработав план, группы можно внедрять.

- Область действия следует определять в соответствии с тем, как будет использоваться группа. Так, глобальные группы рекомендуются для группировки учетных записей пользователей. Локальные доменные и универсальные группы удобны для назначения разрешений доступа к ресурсам. Глобальные группы следует включать в локальные доменные и универсальные группы.
- Добавлять/удалять пользователей из универсальных групп не рекомендуется, поскольку это может сильно увеличить трафик репликации.
- Перед созданием группы в домене убедитесь в наличии у Вас соответствующих прав. Члены групп Administrators и Account Operators данного домена по умолчанию обладают всеми необходимыми разрешениями. Администратор может предоставлять пользователям разрешения на создание групп в доменах или в ОП.
- Имя группы должно быть интуитивным, особенно если администраторы других доменов будут искать его в Active Directory. Если в нескольких доменах есть параллельные группы, убедитесь, что их имена также параллельны. Скажем, если в доменах имеются отдельные группы для менеджеров, система их именования должна быть согласованной, например, Managers USA и Managers Australia.

Создание групп

Для создания групп служит оснастка Active Directory Users And Computers. Их следует создавать в ОП Users или в ОП, созданных специально для групп. В процессе роста и развития организации некоторые группы могут оказаться ненужными. Такие группы надо удалять. Это поможет Вам гарантировать безопасность, т. е. Вы не присвоите разрешения доступа к ресурсам группе, которая больше не используется.

Чтобы создать группу, запустите оснастку Active Directory Users And Computers. В меню Action (Действие) выберите New (Создать), а затем — команду Group (Группа). Откроется диалоговое окно New Object — Group (Новый объект — Группа) (рис. 7-8), параметры которого таковы:

Параметр	Описание
Group Name (Имя группы)	Имя новой группы. В пределах домена, где создается группа, имя должно быть уникальным.
Group Name (preWindows 2000) [Имя группы (пред-Windows 2000)]	Имя группы для **обеспечения** совместимости с предыдущими версиями Windows. Автоматически создается в соответствии с вводимым Вами именем.
Group Scope (Область действия группы)	Область действия группы. Доступные варианты: Domain Local (Локальная в домене), Global (Глобальная) и Universal (Универсальная). Переключатель Universal доступен, только если тип группы — Distribution или если сервер работает в смешанном режиме.
Group Type	Тип группы. Доступные варианты — Distribution (Группа распространения) и Security (Группа безопасности).

Администрирование групп

Оснастка Active Directory Users Anc Computers позволяет добавлять членов в группу, изменять области действия и удалять группы.

Добавление членов в группу

В созданную группу можно добавлять членов — учетные записи пользователей, контакты, другие группы и компьютеры. Компьютеры добавляются в группу для предоставления им доступа к разделяемым ресурсам других систем, например, для удаленного резервного копирования.

Чтобы добавить новых членов, дважды щелкните нужную группу. В диалоговом окне свойств перейдите на вкладку Members (Члены группы) и щелкните кнопку Add (Добавить). Откроется диалоговое окно Select Users, Contacts, Or Computers (Выбор: Пользователи, Контакты и Компьютеры) (рис. 7-10).

Примечание Если домен работает в смешанном режиме, в зависимости от области действия создаваемой группы Вы не всегда сможете добавить в нее другие группы.

Чтобы добавить учетную запись пользователя, контакт, компьютер или группу из определенного домена, выберите нужный домен в списке Look In (Искать в). Кроме того, можно выбрать пункт Entire Directory (Вся папка) и просмотреть все учетные записи и группы хранилища Active Directory. Выберите нужную учетную запись или группу и щелкните кнопку Add (Добавить).

Примечание Несколько учетных записей пользователей или групп можно добавлять по одной или добавить все нужные элементы сразу, выделив их с помощью клавиш Shift или Ctrl. Удерживая Shift, можно выделить последовательный диапазон элементов списка; Ctrl позволяет выделять отдельные группы и учетные записи. Выбрав нужные элементы, щелкните кнопку Add (Добавить).

Просмотрев выбранные элементы и убедившись, что все правильно, щелкните кнопку OK.

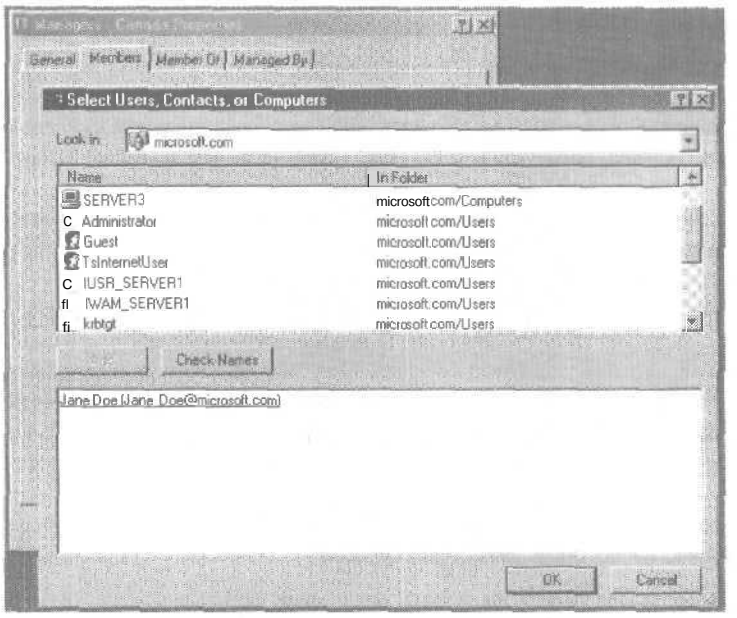


Рис. 7-10. Диалоговое окно Select Users, Contacts, Or Computers (Выбор: Пользователи, Контакты и Компьютеры)

Изменение области действия группы

В процессе развития сети может возникнуть потребность в изменении области действия группы. Например, чтобы предоставить пользователям доступ к ресурсам других доменов, Вам может понадобиться преобразовать имеющуюся локальную доменную группу в глобальную. Изменить область действия группы позволяет вкладка General (Общие) диалогового окна свойств группы,

---

Примечание Изменять область действия группы можно лишь в доменах основного режима. В доменах смешанного режима такая операция не допускается. Кроме того, Windows 2000 не поддерживает изменение области действия универсальной группы, поскольку ограничения на членство и область действия других групп более строги.

Область действия группы можно изменять так:

- **преобразовать глобальную группу в универсальную** — возможно, лишь когда глобальная группа не является членом другой глобальной группы;
- ***преобразовать*** **локальную группу домена в универсальную группу —** возможно, только если локальная группа домена не содержит подобных групп.

Удаление групп

Каждая группа обладает уникальным идентификатором безопасности, SID, повторно задействовать который невозможно. SID в Windows 2000 служит для идентификации групп и присвоенных ей разрешений. Windows 2000 не использует повторно идентификаторы удаленных групп, даже если Вы создадите группу с именем, аналогичным имени удаленной группы. Следовательно, восстановить доступ к ресурсам, воссоздав группу, нельзя.

При удалении группы удаляется лишь сама группа и связанные с ней разрешения. Учетные записи пользователей — членов группы не затрагиваются. Удаляемую группу щелкните правой кнопкой и выберите в контекстном меню команду Delete (Удалить).

Внедрение локальных групп

Локальная группа может включать учетные записи компьютера, на котором она находится. Ее рекомендуется применять для назначения разрешений доступа к ресурсам, расположенным на том же компьютере, чго и группа. Windows 2000 создает локальные группы в локальной БД системы защиты. Локальные группы бывают доменными и изолированными.

Помните следующее.

- Локальные группы домена создаются в хранилище Active Directory и используются всеми контроллерами данного домена. Локальной группе домена можно предоставить разрешения доступа к любому ресурсу на контроллерах домена.
- Изолированные локальные группы создаются на изолированных и рядовых серверах, а также на компьютерах с Windows 2000 Professional. И все же локальные группы можно использовать лишь на той машине, где были созданы. Это значит, что изолированные локальные группы не следует использовать на компьютерах домена. Такие группы не позволяют выполнять централизованное администрирование и не отображаются в хранилище Active Directory. Управление такими группами осуществляется отдельно на каждом компьютере.
- Изолированным локальным группам можно присваивать лишь разрешения доступа к ресурсам того компьютера, на котором находится группа.

Изолированные локальные группы могут включать локальные учетные записи пользователей компьютера, на котором находится группа. Такие группы не могут состоять в других группах.

Создание локальных групп

Изолированные локальные группы позволяет создать оснастка Computer Management. Локальные группы создаются в лапке Croups (Группы) (рис. 7-11). Чтобы создать локальную группу, раскройте в дереве консоли папку Local Users And Groups (Локальные пользователи и группы) и щелкните подпапку Groups (Группы). Затем в меню Action выберите команду New Group (Создать группу). В открывшемся диалоговом окне введите имя и описание группы. Параметры диалоговою окна New Group (Создание группы) описаны ниже.

Параметр	Описание
Group Name (Имя группы)	Уникальное имя локальной группы. Это единственный обязательный параметр. В имени можно использовать любые символы, кроме (\). Длина имени не может превышать 256 символов; однако в некоторых окнах слишком длинные имена отображаться не будут.
Description (Описание)	Описание группы.
Add (Добавить)	Добавить пользователя в список членов группы.
Delete (Удалить)	Удалить пользователя из списка членов группы.
Create (Создать)	Создать группу.

Членов в локальную группу можно добавить как при создании группы, так и после.

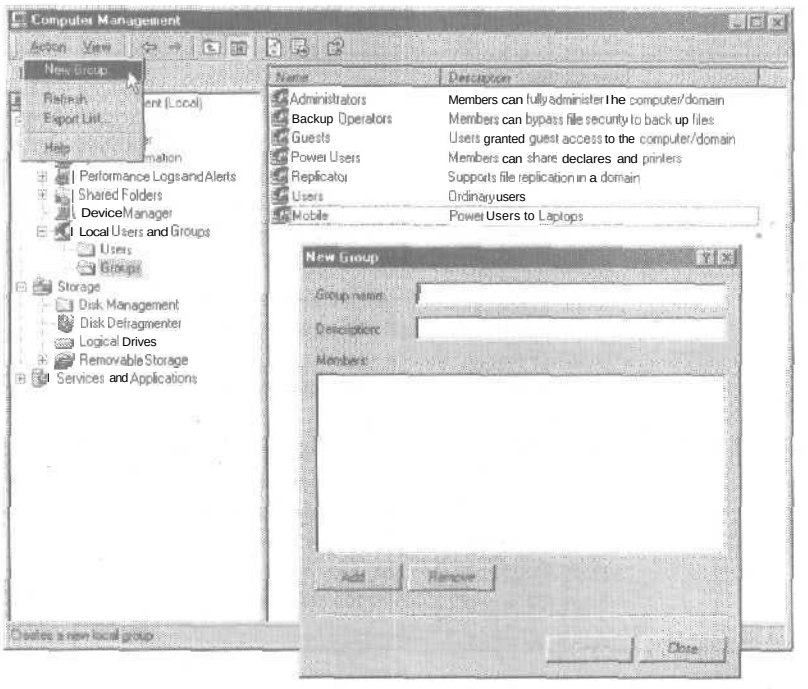


Рис. 7-11. Создание локальной группы на компьютере с Windows 2000 Professional

Встроенные группы

В Windows 2000 четыре типа встроенных групп: глобальные, доменные локальные, изолированные локальные и системные. Встроенные группы обладают предопределенным набором членов и прав. Windows 2000 автоматически создает такие группы, чтобы Вам не приходилось вручную создавать группы и назначать разрешения для часто используемых функций.

Встроенные глобальные группы

Позволяют объединять учетные записи общего типа. Windows 2000 по умолчанию добавляет членов в некоторые встроенные глобальные группы. Вы также можете добавлять в них новых членов, чтобы предоставить им права и разрешения группы.

При создании домена Windows 2000 создает встроенные глобальные группы в хранилище Active Directory. Чтобы присвоить встроенной глобальной группе права, ее можно добавить в локальную группу домена или явно назначить ей нужные права и разрешения.

ОП Users содержит все встроенные группы домена. Ниже перечислены стандартные участники наиболее распространенных встроенных глобальных групп:

Глобальная группа	**Описание**
Domain Users (Пользователи домена)	Windows 2000 автоматически добавляет глобальную группу Domain Users во встроенную локальную группу Users (Пользователи). Учетная запись Administrator (Администратор) по умолчанию включена в группу Domain Users, и Windows 2000 автоматически добавляет в эту группу все новые учетные записи пользователей домена.

(окончание)

Глобальная группа	Описание
Domain Admins (Администраторы домена)	Windows 2000 автоматически добавляет глобальную группу Domain Admins в локальную группу домена Administrators, чтобы члены группы Domain Admins могли выполнять административные задачи на любом компьютере домена. По умолчанию учетная запись Administrator включена в группу Domain Admins.
Domain Guests (Гости домена)	Windows 2000 автоматически добавляет глобальную группу Domain Guests во встроенную локальную группу Guests (Гости). Учетная запись Guest по умолчанию включена в группу Domain Guest; данная учетная запись по умолчанию отключена.
Enterprise Admins (Администраторы предприятия)	В эту группу можно добавить учетные записи пользователей, которым нужны административные привилегии в масштабе всей сети. Встроенная локальная группа Administrators каждого домена по умолчанию включена в глобальную группу Enterprise Admins. По умолчанию учетная запись Administrator также является членом этой глобальной группы.

Примечание Просмотреть участников некоторой группы, а также список групп, в состав которых входит данная группа, позволяют вкладки Members (Члены группы) и Member Of (Член групп) диалогового окна свойств требуемой группы.

Встроенная **локальная** группа **домена**

Windows 2000 создает встроенные локальные группы домена, чтобы предоставить пользователям права и разрешения на выполнение задач в хранилище Active Directory, а также на контроллерах домена. Встроенная локальная группа в целом работает аналогично локальной группе домена, единственное отличие в том, что ее нельзя удалить.

Встроенные локальные группы домена предоставляют добавляемым в них учетным записям пользователей и глобальным группам набор предопределенных прав и разрешений. Наиболее распространенные встроенные локальные группы, а также привилегии, которыми обладают их члены, таковы;

Глобальная группа	Члены группы вправе
Account Operators (Операторы учета)	Создавать, удалять и изменять права групп и учетных записей пользователей. Члены группы не имеют разрешения на изменение группы **Administrators и** любых групп **операторов.**
Server Operators (Операторы сервера)	Предоставлять в совместное использование дисковые ресурсы, архивировать и восстанавливать файлы на контроллере домена.
Print Operators (Операторы печати)	Настраивать и управлять сетевыми принтерами на контроллерах домена.

(окончание)

Глобальная группа	Члены группы вправе
Administrators (Администраторы)	Выполнять все административные задачи на любых контроллерах домена, включая сам домен. По умолчанию членами данной локальной группы являются учетная запись Administrator, глобальные группы Domain Admins и Enterprise Admins.
Backup Operators (операторы архива)	Архивировать и восстанавливать все контроллеры домена при помощи утилиты Windows Backup (Архивация).
Guests (Гости)	Обращаться лишь к тем ресурсам и выполнять лишь те задачи, на которые у них имеются разрешения. Члены группы не могут вносить постоянные изменения в конфигурацию рабочего стола. По умолчанию членами этой группы являются учетная запись Guest и глобальная группа Domain Guests. При установке некоторые службы автоматически добавляют пользователей в эту локальную группу. Например, службы Microsoft Internet Information Services (IIS) автоматически добавляют во встроенную группу Guests учетные записи анонимных пользователей.
Users (Пользователи)	Обращаться лишь к тем ресурсам и выполнять лишь те задачи, на которые у них имеются разрешения. Члены группы не могут вносить постоянные изменения в конфигурацию рабочего стола. По умолчанию членами этой группы являются группа Domain Users, специальные группы Authenticated Users (Прошедшие проверку) и INTERACTIVE (Интерактивные). Поддержка системных групп осуществляется Windows 2000; удалить их нельзя. Группу Users рекомендуется применять для предоставления всем учетным записям домена прав и разрешений, которыми должен обладать каждый пользователь.

Встроенные локальные группы

На всех изолированных и рядовых серверах и компьютерах с Windows 2000 Professional есть встроенные локальные группы. Они предоставляют разрешения на выполнение задач (восстановление и архивирование файлов, изменение системного времени, администрирование ресурсов системы и др.) на отдельном компьютере. Windows 2000 помещает встроенные локальные группы в папку Groups (Группы) оснастки Computer Management. Как и встроенные доменные локальные, удалить встроенные недоменные локальные группы нельзя.

Права, которыми обладают члены встроенных локальных групп, таковы:

Локальная группа	Члены группы вправе
Users (Пользователи)	Обращаться лишь к тем ресурсам и выполнять лишь те задачи, на которые у них есть соответствующие разрешения. Члены группы не могут вносить постоянные изменения в конфигурацию рабочего стола. По умолчанию Windows 2000 добавляет в группу Users все новые локальные учетные записи пользователей. Если рядовой сервер или компьютер с Windows 2000 Professional присоединяются к домену, Windows 2000 добавляет в локальную группу Users глобальную группу Domain Users и специальные группы Authenticated Users и INTERACTIVE.
Administrators (Администраторы)	Выполнять на компьютере любые административные задачи. Встроенная учетная запись Administrator компьютера по умолчанию является членом локальной группы Administrators. Если рядовой сервер или компьютер с Windows 2000 Professional присоединяется к домену, Windows 2000 добавляет в локальную группу Administrators глобальную группу Domain Admins.
Guests (Гости)	Обращаться лишь к тем ресурсам и выполнять лишь те задачи, на которые у них имеются разрешения. Члены группы не могут вносить постоянные изменения в конфигурацию рабочего стола. Встроенная учетная запись Guest компьютера по умолчанию является членом локальной группы Guests; при установке эта учетная запись отключается. Если рядовой сервер или компьютер с Windows 2000 Professional присоединяется к домену, доменные группы в эту группу не добавляются.
Backup Operators (Операторы архива)	Архивировать и восстанавливать систему с помощью утилиты Windows Backup.
Power Users (Опытные пользователи)	Создавать и изменять учетные записи пользователей компьютера, открывать доступ к ресурсам.
Replicator (Репликатор)	Настраивать службы репликации файлов.

Встроенные системные группы

На всех Windows 2000-компьютерах зсть встроенные системные группы (в Windows NT – специальные группы). Системные группы не имеют определенного списка членов, который можно было бы изменять; в разное время состав членов таких групп может различаться в зависимости от метода доступа пользователя к ресурсу или компьютеру. При администрировании системные группы недоступны, однако они отображаются при назначении прав и разрешений доступа к ресурсам. Состав системных групп в Windows 2000 основан на способе доступа к компьютеру, а не на том, какие пользователи работают с компьютером. Наиболее распространены встроенные системные группы:

Системная группа	Описание
Everyone **(Все)**	Включает всех пользователей, обращающихся к компьютеру. При назначении разрешений группе Everyone и включении учетной записи Guest будьте особенно осторожны. Windows 2000 аутентифицирует пользователя без действительной учетной записи как гостя (Guest). Такой пользователь автоматически получает все права и привилегии, которыми обладает группа Everyone.

(*окончание*)

Системная группа	Описание
Authenticated Users (Прошедшие проверку)	Включает всех пользователей компьютера и службы Active Directory, обладающих действительными учетными записями. Для предотвращения анонимного доступа к ресурсам вместо группы Everyone используйте эту группу.
Creator Owner (Создатель-владелец)	Включает учетную запись пользователя, создавшего или вступившего во владение ресурсом. Если ресурс создан членом группы Administrators, владельцем ресурса считается группа Administrators.
Network (Сеть)	Включает всех пользователей, находящихся за другими компьютерами сети и подключенных к общему ресурсу компьютера, на котором размещается группа.
Interactive (Интерактивные)	Включает учетную запись пользователя, зарегистрировавшегося в системе. Члены группы Interactive могут подключаться к ресурсам компьютера, за которым они физически находятся. Пользователь регистрируется в системе и обращается к ресурсам, «взаимодействуя» с компьютером.
Anonymous Logon (Анонимный вход)	Включает все учетные записи, не аутентифицированные Windows 2000.
Dialup (Удаленный доступ)	Включает всех пользователей, подключенных в текущий момент поудаленномуподключению.

Упражнение 4: изменение режима домена

Измените режим своего домена с помощью оснастки Active Directory Users And Computers.

► **Задание 1:** переведите **домен из смешанного режима в основной**

По умолчанию Windows 2000 Server работает в смешанном режиме. Чтобы задействовать все функции работы с группами, доступные в Windows 2000 Server, домен должен работать в основном режиме. Выполняйте упражнение на Server01.

1. Зарегистрируйтесь на ServerOl как Administrator (Администратор) с паролем password.
2. Откройте оснастку Active Directory Users And Computers.
3. В дереве консоли выберите свой домен и затем в меню Action (Действие) — команду Properties (Свойства).

   Откроется диалоговое окно свойств microsoft.com.

   В настоящий момент домен работает в смешанном режиме. Обратите внимание на предупреждение об изменении режима домена.
4. Щелкните кнопку Change Mode (Изменить режим).

   Active Directory предупредит о невозможности отмены изменений.

   Щелкните кнопку Yes (Да).

   В окне свойств microsoft.com будет показано, что домен был переведен в основной режим.
5. Щелкните кнопку OK, чтобы закрыть окно свойств microsoft.com.

   Active Directory сообщит об успешном изменении режима домена и укажет, что репликация новой информации на другие контроллеры домена может занять более 15 минут.

6. Щелкните кнопку OK.
7. Не закрывайте оснастку Active Directory Users And Computers — она нужна для выполнения упражнения 5.

Упражнение 5: создание групп

Вы создадите глобальную группу защиты и добавите в нее членов — две ранее созданные учетные записи Jane Doe и John Smith. Затем Вы создадите локальную группу домена и назначите ей разрешения доступа к отчетам о продажах. После этого Бы предоставите членам глобальной группы защиты доступ к отчетам о продажах, добавив эту группу в локальную группу домена. Выполняйте упражнение на Server01.

► Задание 1: создайте глобальную группу, добавьте участников и организуйте учетные записи пользователей

Создайте глобальную группу защиты, добавьте в нее членов и переместите пользователя из одного организационного подразделения (ОП) в другое.

1. Убедитесь, что оснастка Active Directory Users And Computers открыта и в фокусе.
2. В дереве консоли щелкните узел ОП Sales.

   На правой панели появится учетная запись пользователя Jane Doe.
3. В меню Action выберите New (Создать), а затем — команду Group.

   Откроется диалоговое окно New Object — Group (Новый объект — Группа).

   Когда выбрана группа безопасности, доступна универсальная область действия. Это связано с тем, что служба каталогов Active Directory работает в основном режиме.
4. Убедитесь, что выбраны переключатели Global (Глобальная) и Security (Группа безопасности).
5. В поле Group Name (Имя группы) введите Sales и щелкните OK.

   На правой панели узла появится новая группа.
6. На правой панели дважды щелкните группу Sales.

   Откроется диалоговое окно Sales Properties (Свойства: Sales).
7. Перейдите на вкладку Members (Члены группы).
8. Щелкните кнопку Add (Добавить).

   Откроется диалоговое окно Select Users, Contacts, Computers, Or Groups (Выбор: Пользователи, Компьютеры, Контакты или Группы); в списке Look In (Искать в) будет выбрано microsoft.com.
9. В списке учетных записей, групп *л* компьютеров щелкните Jane_Doe и, удерживая клавишу Ctrl, щелкните John_Smith.

   Будут выбраны обе учетные записи. Учетная запись Jane Doe находится в ОП microsoft.com/Sales, а John Smith — в ОП microsoft.com/Users.
10. Щелкните кнопку Add (Добавить).

    Учетные записи Jane Doe и John Smith стали членами глобальной группы защиты Sales.
11. Щелкните кнопку OK,
12. Снова щелкните кнопку OK, чтобы закрыть диалоговое окно Sales Properties (Свойства: Sales).

    В организационных целях Вы решили переместить учетную запись John Smith в ОП Sales.
13. Щелкните ОП Users.
14. На правой панели щелкните учетную запись John Smith.

15. В меню Action (Действие) выберите команду Move (Переместить).
    Откроется одноименное окно.
16. Выберите ОП Sales и щелкните кнопку OK.
    Учетная запись John Smith больше не отображается в правой панели ОП Users.
17. В дереве консоли щелкните ОП Sales.
    В правой панели отображены учетные записи John Smith и Jane Doe и глобальная группа безопасности Sales.
18. Дважды щелкните глобальную группу Sales. Откроется диалоговое окно Sales Properties (Свойства: Sales).
19. Перейдите на вкладку Members (Члены группы).
    Учетная запись John Smith по-прежнему член группы Sales, но находится теперь в папке microsoft.com/Sales.
20. Щелкните кнопку OK.

► **Задание 2: создайте и используйте локальную группу домена**

Создайте локальную группу домена для предоставления доступа к отчетам о продажах. В нее Вы добавите глобальную группу безопасности, созданную на этапе 1.

1. Щелкните правую панель консоли, чтобы снять выделение с группы Sales.
2. В меню Action выберите New, а затем — команду Group.
   Откроется диалоговое окно New Object — Group.
3. В поле Group Name (Имя группы) введите **Reports.**
4. Щелкните переключатели Security (Группа безопасности) и Domain Local (Локальная в домене).
5. Щелкните кнопку OK.
   На правой панели для ОП Sales появится локальная группа домена.
6. На правой панели дважды щелкните группу Reports,
   Откроется диалоговое окно Reports Properties (Свойства: Reports).
7. Перейдите на вкладку Members (Члены группы).
8. Щелкните кнопку Add (Добавить).
   Откроется диалоговое окно Select Users, Contacts, Computers, Or Groups.
9. В списке Look In (Искать в) выберите пункт Entire Directory (Вся папка).
   Будут отображены учетные записи и группы всех доменов, а также расположение этих учетных записей и групп.
10. В списке учетных записей, групп и компьютеров щелкните заголовок Name (Имя).
    Поле Name (Имя) будет отсортировано по алфавиту в убывающем порядке.
11. Снова щелкните этот заголовок, чтобы отсортировать поле по алфавиту в возрастающем порядке.
12. В списке учетных записей, групп и компьютеров выделите ОП Sales и щелкните кнопку Add (Добавить). Щелкните кнопку OK.
    Группа Sales стала членом доменной локальной группы Reports.
13. Щелкните кнопку OK.
14. Закройте оснастку Active Directory Users And Computers.

► **Задание 3: назначьте разрешения NTFS**

В главе 4 рассказывалось о разрешениях NTFS. Вы назначите локальной группе домена Reports разрешения NTFS и проверите доступ к папке sales. Выполняйте упражнение на Server01.

1. Создайте на диске C: папку с именем Dept.
2. Сделайте эту папку общей с именем ресурса Dept, а в поле Comment (Комментарий) введите **Department** share.

   Для общего ресурса **задавать разрешения не** надо, **так как папка Dept создана на томе NTFS.**
3. Создайте в папке Dept подкаталог Sales.
4. Выделите папку Sales.
5. В меню File (Файл) выберите команду Properties (Свойства).

   Откроется диалоговое окно Sales Properties (Свойства: Sales).
6. Перейдите на вкладку Security (Безопасность).

   Системной группе Everyone (Все) предоставлены полные права управления данной папкой.
7. Снимите флажок Allows Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект).

   Появится сообщение Security (Безопасность) с описанием доступных вариантов выбора.
8. Щелкните кнопку Remove (Удалить).

   Откроется диалоговое окно Sales Properties (Свойства: Sales).
9. Щелкните кнопку Add (Добавить).

   Откроется диалоговое окно Select Users, Computers, Or Group.
10. В списке Look In (Искать в) выберите пункт Entire Directory (Вся папка).
11. В списке учетных записей, групп и компьютеров выделите Reports и щелкните кнопку Add.
12. Щелкните кнопку OK.

    В диалоговом окне свойств папки Sales показывается, что локальной группе Reports предоставлены разрешения Read & Execute (Чтение и выполнение), List Folder Contents (Просмотр содержимого папки) и Read (Чтение).
13. Пометьте флажок Write (Запись) и щелкните кнопку OK.
14. Закройте окно Dept и завершите с;еанс Administrator (Администратор).
15. Зарегистрируйтесь в системе как Jane Doe с паролем student и откройте в окне My Computer (Мой компьютер) папку C:\Dept\SaIes.
16. В меню File выберите New, а затем — Text Document (Текстовый документ).

    В окне Sales появится файл New Text Document (Новый текстовый докуменг).
17. Дважды щелкните этот файл.

    Откроется окно программы Notepad (Блокнот).
18. Введите несколько символов и закройте Notepad.

    Появится запрос на сохранении изменений.
19. Щелкните кнопку Yes (Да).
20. Закройте окно Sales.
21. Завершите сеанс Jane_Doe и зарегистрируйтесь как Bob_Train без пароля.

    В случае ошибки убедитесь, что Вы пытаетесь зарегистрироваться в интервал времени, когда пользователю Bob Train разрешено работать в системе. Вы задали этот интервал в одном из предыдущих упражнений данной главы.
22. Попробуйте обратиться к папке C:\Dept\Sales.

    Сообщение Dept известит об отказе и доступе.

    Дело в том, что Bob Train — не член глобальной группы Sales, которая в свою очередь включена в доменную локальную группу Report. Доступ к локальным папкам тоже

невозможен, так как разрешения NTFS распространяются и на сетевой, и на локальный доступ.

23. Щелкните кнопку OK и закройте окно Dept.
24. Завершите сеанс Bob Train.

Резюме

Группа представляет собой набор учетных записей пользователей, контактов, компьютеров и других групп. В Windows 2000 два типа групп: безопасности и распространения. В Windows 2000 доступны только группы безопасности, применяемые для назначения разрешений и предоставления доступа к ресурсам. Приложения используют группы распространения как списки пользователей для осуществления функций, не связанных с системой защиты. Группы классифицируются не только по типам, но и по области действия. По этому признаку они делятся на глобальные, универсальные и доменные локальные. Локальные группы безопасности домена используются в основном для назначения разрешений доступа к ресурсам, а глобальные — для объединения пользователей с одинаковыми требованиями доступа к сети. Универсальные группы применяются для назначения разрешений доступа к ресурсам разных доменов. Область действия группы определяет состав ее членов. Правила членства указывают, кого может включать группа и в какие группы она может входить. Для создания групп служит оснастка Active Directory Users And Computers. Кроме того, она позволяет администрировать группы; добавлять в них новых членов, изменять области ее действия и удалять ее. Для создания автономных локальных групп служит оснастка Computer Managemen.

Занятие 4. Администрирование групповой политики

Групповые политики — средство совершенствования и централизации управления настройкой рабочего стола пользователя. Их можно применять для управления программами, доступными пользователям и появляющимися на его рабочем столе или в меню Start (Пуск).

Обычно настраивать групповые политики Вам не надо; это задача администраторов групповой политики. Групповые политики обычно настраиваются для всего домена или сети и служат для внедрения корпоративных политик. Они влияют на учетные записи пользователей, группы, компьютеры и ОП, которыми Вы управляете.

Изучив материал этого занятия, Вы сможете:

- ✓ объяснить структуру групповых политик, включая их объекты, контейнеры и шаблоны;
- ✓ объяснить иерархию применения групповых политик, включая правила наследования и методы модификации наследования политик;
- ✓ создавать объект групповой политки и задавать его параметры в оснастке Active Directory Users And Computers;
- ✓ настраивать групповые политики для компьютеров и пользователей из оснастки Group Policy.

Продолжительность занятия — около 90 минут.

Введение в групповые политики

Групповые политики представляют собой набор параметров конфигурации, которые администратор групповой политики применяет к одному или нескольким объектам в хранилище Active Directory. С их помощью он управляет рабочей средой пользователей в домене и контролирует рабочую среду пользователей определенного ОП, Групповые политики можно установить на уровне сайта из оснастки Active Directory Sites And Services (Active Directory — сайты и службы).

Групповая политика состоит из параметров, управляющих поведением объекта и его дочерних объектов. Администратор групповой политики может обеспечить пользователей полностью настроенным рабочим столом. Этот рабочий стол может включать настроенное меню Start (Пуск), автоматически настроенные приложения и ограничения доступа к файлам, папкам и системным параметрам Windows 2000. Групповая политика может также влиять на разрешения, предоставленные учетным записям пользователей и групп.

Между групповыми политиками и локальными потребностями могут возникать конфликты, например, когда политика запрещает пользователю доступ к ресурсу. Для разрешения конфликта надо обратиться к администратору групповой политики. Однако делать это нужно не всегда — Вы можете разблокировать заблокированную учетную запись. Имейте, однако, в виду, что Вам не следует выполнять задания, переопределенные групповой политикой, если она переопределяет параметры профиля.

Преимущества групповой политики

Совокупная стоимость владения (total cost of ownership, TCO) — это стоимость управления распределенными сетями персональных компьютеров. Недавние исследования TCO от-

мечают снижение производительности пользователей как одну из главных статей расходов корпораций. Зачастую это случается из-за ошибки пользователя, например модификации файлов системной конфигурации и как следствие вывода компьютера из строя; она может быть вызвана большим количеством ненужных приложений, доступных пользователю.

Вы можете снизить TCO сети, применив групповые политики для создания управляемой среды рабочего стола, отвечающей потребностям пользователя и его опыту.

Обеспечение безопасности среды пользователя

Вы можете создать на компьютере заблокированную среду. Задав соответствующие параметры групповой политики для определенных пользователей в сочетании с разрешениями NTFS, обязательными профилями и другими средствами безопасности Windows 2000, Вы можете предотвратить установку пользователями ПО и их доступ к запрещенным программам или данным. Вы можете также запретить пользователям удалять файлы, необходимые для правильного функционирования приложений или ОС.

Защита среды пользователя

Групповая политика позволяет защитить среду пользователя, настроив:

- автоматическое включение приложений в меню Start (Пуск) для пользователя;
- распространение приложений, чтобы пользователи легко находили их в сети и устанавливали;
- доставку файлов или ярлыков в нужные места сети или в папку на компьютере пользователя;
- автоматизацию выполнения заданий или программ в момент входа или выхода пользователя или в момент включения или выключения компьютера;
- переназначение папок на сетевые ресурсы для увеличения надежности хранения данных.

Примечание О групповых политиках см. также документы \chap07\articles\Outline for Group Policy Design Readiness White Paper 3.doc и \chap07\articles\GroupPolicyWhitePaper\WhitePaperBeta3.doc) на прилагаемом компакт-диске.

Типы групповых политик

Групповые политики влияют на множество сетевых компонентов и объектов Active Directory. Типы групповых политик таковы:

Тип групповой политики	Описание
Конфигурация программ	Указывает приложения, к которым пользователь может получить доступ. Этот тип позволяет автоматически **устанавливать** приложения: **назначением приложения** — групповая политика автоматически устанавливает или обновляет приложения на клиентских компьютерах или обеспечивает пользователя связью с приложением, которое он не может удалить; **публикацией приложения** — администратор групповой политики публикует приложения в Active Directory, затем они появляются в списке компонентов, которые пользователь может установить с помощью команды Add/Remove Programs в Control Panel; пользователь может удалить это приложение.

(окончание)

Тип групповой политики	Описание
Сценарии	Позволяет администраторам групповой политики определять сценарии и командные файлы, выполняемые в определенное время, например при запуске или остановке системы или в момент входа или выхода пользователя. Сценарии автоматизируют повторяющиеся задания, такие как подключение сетевых дисков.
Службы удаленной установки (Remote Installation Services, RIS)	Управляет параметрами установки RIS, предлагаемыми мастером клиентской установки.
Параметры безопасности	Позволяет администраторам групповой политики ограничивать доступ пользователей к файлам и папкам, конфигурировать учетные ограничения (например, сколько раз пользователь может ввести неверный пароль, до того как Windows 2000 заблокирует его учетную запись), настраивать локальную политику (например, права и аудит пользователя), управлять сервисной работой служб, ограничивать доступ к реестру и журналу событий, настраивать доступ к открытому ключу и конфигурировать политику безопасности IP (IPSec).
Административные шаблоны	Включает групповые политики, позволяющие регулировать параметры реестра в отношении поведения и вида рабочего стола, включая компоненты ОС и приложения.
Перенаправление папок	Позволяет перенаправлять папки Windows 2000 с места, определенного профилем пользователя по умолчанию, на новое место в сети, где ими можно будет управлять централизованно.

Структура групповой политики

Групповые политики (group policies) — это наборы параметров конфигурации, применяемых к одному или нескольким объектам в хранилище Active Directory. Эти параметры находятся внутри *объекта групповой политики* (group policy object, GPO), который хранит данные групповой политики в контейнерах и шаблонах.

Объекты групповой политики

Содержат параметры узлов, доменов и ОП, которые записываются в хранилище Active Directory в *контейнер групповой политики* (group policy container. GPC). Кроме того, GPO хранят данные групповой политики в структуре папок — *шаблоне групповой политики* (group policy template, GPT). Внутренняя структура GPO чаше всего скрыта от администратора.

Один или несколько объектов GPO могут быть применены к сайту, домену или ОП. Несколько контейнеров в хранилище Active Directory могут быть связаны с одним и тем же GPO, а один контейнер может иметь более одного GPO, связанного с ним. Область действия GPO обусловлена членством в группах безопасности.

Небольшие и редко меняющиеся данные групповой политики хранятся в GPC. Большие и часто меняющиеся данные групповой политики хранятся в GPT.

Локальные объекты групповой политики

Существуют на каждом компьютере с Windows 2000, и по умолчанию в них сконфигурированы только параметры безопасности. Локальный GPO хранится в папке %systemroot%\System32\GroupPolicy и имеет следующие разрешения ACL:

- Administrators (Администраторы) — Full Control (Полный доступ);
- SYSTEM (Система) — Full Control;
- Authenticated Users (Прошедшие проверку) — Read & Execute (Чтение и выполнение), List Folder Contents (Список содержимого папки) и Read (Чтение).

Примечание Группы SYSTEM и Authenticated Users — системные.

Контейнеры групповой политики

Это объекты Active Directory, хранящие свойства GPO и включающие подконтейнеры для компьютера и данных групповой политики пользователя. Сведения о версиях, содержащиеся в GPC, обеспечивают синхронизацию информации, хранящейся в GPC, с информацией GPT. GPC содержит также информацию о состоянии, указывающую, активен GPO или нет.

GPC содержит данные хранилища классов Windows 2000 для развертывания приложений. *Хранилище классов* (class store) — это основанное на сервере хранилище всех приложений, интерфейсов и API, обеспечивающих публикацию и назначение приложений.

Шаблоны групповой политики

Шаблон GPT является структурой папки %systemroot%\SYSVOL\sysvol\<*имя_домена*>\Policies на контроллерах доменов. GPT является контейнером, хранящим параметры политики для административных шаблонов, безопасности, ПО и сценариев.

Структура GPT

При создании GPO создается и соответствующая структура папок GPT. Имя папки, присваиваемое GPO, является GUID созданного объекта GPO. Так, если созданный GPO ассоциируется с доменом microsoft.com, результирующая папка GPT будет иметь имя:

```
%systemroot%\SYSVOL\sysvol\microsoft.com\Policies\{45265FA6-554F-4F74-97CC-
61B4663DAE61}
```

Примечание Приведенный выше GUID является примером.

Содержимое GPT

По умолчанию в GPT содержатся подкаталоги User и Machine и файл Gpt.ini. По мере создания и модификации политик создаются дополнительные папки. Структура папки зависит от настроенных Вами групповых политик. В структуре GPT часто содержатся подкаталоги:

Подкаталог	Содержимое
\Adm	Файлы шаблона .adm, связанные с определенным GPT. Текстовые ADM-файлы обрабатываются Windows 2000 для внесения изменений в реестр.
\User	Файл Registry.pol с параметрами реестра для пользователей.
\User\Applications	Файлы оповещения (файлы .aas), используемые программой Windows Installer для публикации пакетов ПО для пользователей.

(окончание)

Подкаталог	Содержимое
\User\Documents & Settings	Любые файлы, развертываемые на рабочем столе пользователя в рамках GPT.
\User\Scripts	Подкаталоги Logon и Logoff.
\User\Scripts\Logon	Сценарии и связанные с ними файлы для сценариев входа.
\User\Scripts\Logoff\	Сценарии и связанные с ними файлы для сценариев выхода.
Machine	Файл Registry.pol с параметрами реестра для применения к компьютерам.
\Machine\Appliations	Файлы оповещения (файлы .aas), используемые Windows Installer для публикации пакетов ПО на компьютеры.
\Machine\Documents & Settings	Любые файлы для развертывания на всех рабочих столах для всех пользователей, которые подключаются к этому компьютеру как часть этого GPT.
\Machine\Microdoft\ WindowsNT\SecEdit	Файл GptTmpl.ini редактора Security Editor.
\Machine\Scripts	Подкаталоги Startup и Shutdown.
\Machine\Scripts\	Сценарии и связанные с ними файлы для сценариев запуска.Startup
\Machine\Scripts\ Shutdown	Сценарии и связанные с ними файлы для сценариев выключения.

Файл Gpt.ini

В корневой папке каждого GPT находится файл Gpt.ini. Он может содержать записи:

- **Version=*x***, где ***x*** — номер версии объекта GPO; номер версии начинается с 0, когда Вы впервые создаете GPO, и автоматически увеличивается на 1 каждый раз, когда Вы изменяете GPO;
- **Disabled=*y***, где *y* принимает значение 0 или 1 и относится только к локальному GPO; этот переключатель показывает, активизирован ли локальный GPO; для всех остальных GPO информация о состоянии хранится в GPC, расположенном в хранилище Active Directory.

Файл Registry.pol

Хранится в подкаталоге User, загружается и применяется к разделу реестра HKEY_CURRENT_USER в момент регистрации пользователя; в подкаталоге Machine загружается и применяется к разделу реестра HKEY LOCAL_MACHINE при загрузке компьютера.

Формат файлов Registry.pol отличается от файлов, создаваемых в System Policy Editor для Windows 9x или Windows NT 4.0. Файлы, созданные с помощью более ранних версий редактора политики, неприменимы к Windows 2000-компьютерам, и файлы, созданные в оснастке Group Policy (Групповая политика), неприменимы к компьютерам со старыми ОС Windows.

Применение групповой политики

Перед созданием групповой политики Вы должны создать GPO. Из них Вы сможете редактировать групповую политику, управлять разрешениями и их наследованием.

Создание GPO

Первый шаг создания групповой политики — создание или открытие GPO. Вы можете создать объект групповой политики для домена или ОП, используя оснастку Active Directory Users And Computers. Объект групповой политики для сайта можно создать с помощью оснастки Active Directory Sites And Services. В обоих случаях процесс одинаков.

Для создания объекта групповой политики откройте окно свойств сайта, домена или ОП и перейдите на вкладку Group Policy. Щелкните кнопку New (Создать) и введите имя объекта (рис. 7-12).

Примечание Вы можете добавить существующий GPO, щелкнув кнопку Add (Добавить) и выбрав GPO из сайтов, доменов и ОП.

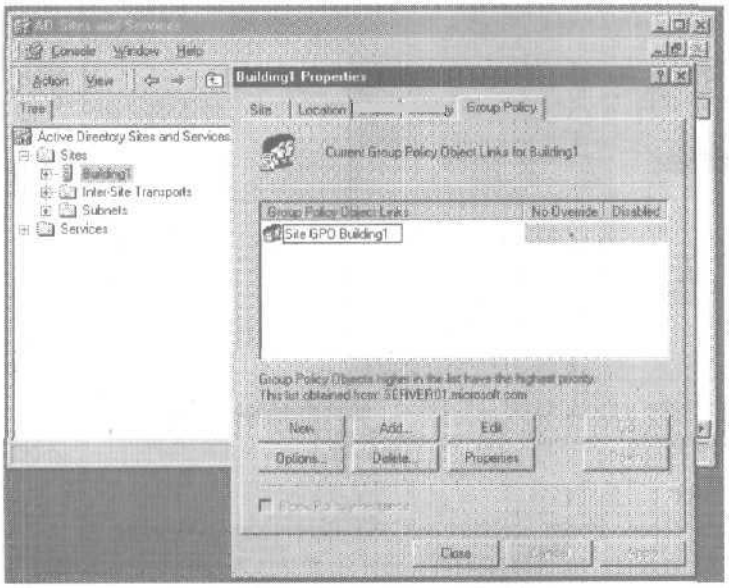


Рис. 7-12. Создание объекта групповой политики для сайта Building1

Оснастка Group Policy

Оснастка Group Policy (Групповая политика) — основной инструмент администратора для определения и управления поведением программ, сетевых ресурсов и ОС для пользователей и компьютеров в организации. В среде Active Directory групповые политики применяются к пользователям или компьютерам на основе их членства в сайтах, доменах или ОП.

Создав GPO, Вы можете из оснастки Group Policy задать параметры групповой политики для компьютеров и учетных записей пользователей (рис. 7-13).

Интерфейс оснастки Group Policy

Оснастка включает в себя узлы Computer Configuration (Конфигурация копьютера) и User Configuration (Конфигурация пользователя). Каждый узел отображает расширения;

- Software Settings (Конфигурация программ);
- Windows Settings (Конфигурация Windows);
- Administrative Templates (Административные шаблоны).

Узел Computer Configuration

Папки узла Computer Configuration содержат параметры среды пользователя или применения правил для компьютеров в сети. Политики Computer Configuration применяются при инициализации ОС. Если назначить компьютерам пользовательские политики, они будут применяться ко всем пользователям этих компьютеров независимо от ОП, членами которого они являются.

Узел User Configuration

Содержит папки с параметрами среды пользователя или применения правил для пользователей в сети.

Они включают все определенные пользователем политики, например, вид рабочего стола, параметры приложений, сценарии входа и выхода, назначенные и опубликованные приложения. Политики User Configuration (Конфигурация пользователя) применяются при регистрации пользователя на компьютере.

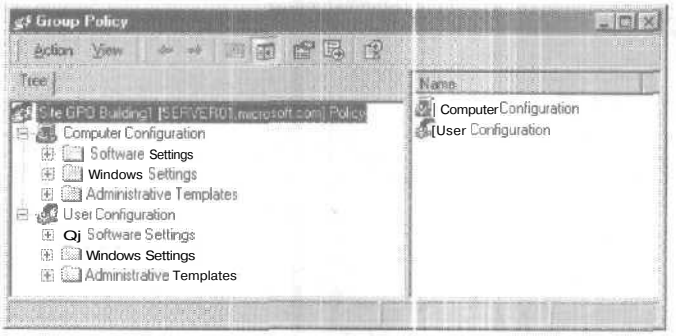


Рис. 7-13. Оснастка Group Policy (Групповая политика), появляющаяся после щелчка кнопки Edit (Изменить), как показано на рис. 7-12

Работа с оснасткой Group Policy

Каждый экземпляр оснастки Group Policy зависит от GPO. Вы можете добавить эту оснастку для определенного GPO в консоль MMC, чтобы использовать как самостоятельный инструмент. Это позволяет Вам добавлять оснастку для каждого GPO, которым Вы хотите управлять. Можно также открыть оснастку Group Policy для определенного GPO через узел, домен или ОП, где расположен GPO. Наконец, Вы можете редактировать локальный GPO с помощью Gpedit.msc.

Создание консоли MMC

Консоль MMC позволяет создать инструмент, содержащий оснастку Group Policy для каждого GPO, которым Вы хотите управлять. Открыв интерфейс MMC, добавьте Group Policy как изолированную оснастку. При этом выберите связанный с ней GPO. Вы можете добавить локальный GPO (по умолчанию) или GPO из сайтов, доменов или ОП Вашей сети (рис. 7-14). Можно также просмотреть локальный GPO на любом компьютере в Вашем домене. Добавив оснастку Group Policy для каждого GPO, которым Вы собираетесь управлять, сохраните консоль как файл .mmc. Впоследствии Вы сможете в любой момент открыть этот файл для управления обьектами GPO, которые Вы добавили в консоль. Вы можете также добавлять или удалять GPO по мере надобности.

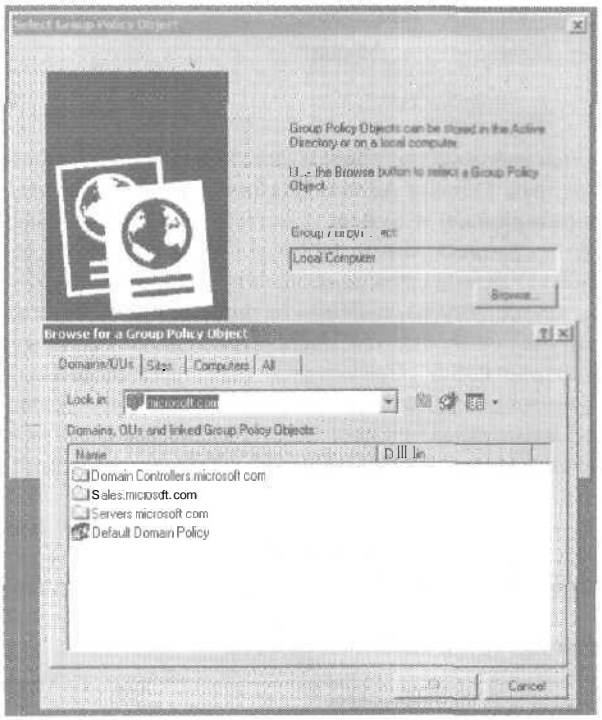


Рис. 7-14. Просмотр групповых политик в домене microsoft.com

*Редактирование GPO в сайтах, **доменах и** ОП*

Для создания и редактирования GPO откройте оснастку Group Policy для определенного GPO из сайта, домена или ОП. Для сайтов используйте оснастку Active Directory Sites And Services, а для доменов — Active Directory Users And Computers. Откройте окно свойств сайта, домена или ОП и выберите вкладку Group Policy. Выберите GPO, которым Вы хотите управлять, и щелкните кнопку Edit (Изменить). Эта операция запускает оснастку Group Policy для выбранного объекта.

Консоль Gpedit.msc

Вы можете редактировать локальный GPO, используя консоль Gpedit.msc. В меню Start (Пуск) выберите команду Run (Выполнить), введите **gpedit.msc** и щелкните кнопку OK. Так запускается оснастка Group Policy для GPO на локальном компьютере.

Вы можете удаленно управлять групповой политикой, используя параметры gpcomputer: <*имя_компьютера*>или gpobject вместе с Gpedit.msc. Переменная *имя_компьютера*, используемая с gpcomputer, может быть NetBIOS- или DNS-именем. Для просмотра и конфигурирования GPO домена для Server01 в домене microsoft.com можно ввести:

```
gpedit.msc /gpcomputer:"server01"
```

или

```
gpedit.msc /gpcomputer:"server01.microsoft.com"
```

Параметр gpcomputer предназначен для отображения GPO домена. Параметр gpobject требует путь ADSI и может открыть любой GPO в хранилище Active Directory. Так, чтобы открыть GPO с GUID 45265FA6-554F-4F74-97CC-61B4663DAE61 в домене microsoft.com можно ввести:

```
gpedit.msc/gpobject:"LDAP://CN={45265FA6-554F-4F74-97CC-
61B4663DAE61},CN=Policies,CN=System,DC=microsoft,DC=com"
```

Разрешения GPO

При создании GPO к объекту добавляется набор групп, причем каждая сконфигурирована с набором свойств. По умолчанию группам Domain Admins (Администраторы домена), Enterprise Admins (Администраторы предприятия) и System (Система) для GPO предоставлены разрешения Read (Чтение), Write (Запись), Create All Child Objects (Создание дочерних объектов) и Delete All Child Objects (Удаление дочерних объектов). Системной группе Creator Owner (Создатель-владелец) также даны разрешения на управление дочерними объектами внутри GPO. Системная группа Authenticated Users (Прошедшие проверку) имеет доступ Read (Чтение) и Apply Group Policy (Применение групповой политики). Только группа Authenticated Users по умолчанию имеет атрибут Apply Group Policy. Члены всех групп, кроме Authenticated Users, могут редактировать GPO. Параметры политики, содержащиеся в GPO, не применяются к членам группы, не имеющей разрешения Apply Group Policy.

Администраторы могут определять, какие группы пользователей и компьютеров имеют доступ для применения групповой политики к объекту. Группы с разрешениями Apply Group Policy и Read для GPO получают сконфигурированные параметры групповой политики, содержащиеся в объекте.

В таблице приведен список стандартных групп GPO и их свойств:

Группа безопасности	Параметры по умолчанию
Authenticated Users (Прошедшие проверку)	Read, Apply Group Policy (AGP)
Creator **Owner** (Создатель-владелец)	Дочерним **объектам** и свойствам **внутри GPO присвоены специальные** разрешения Object **и Attribute**
Domain Admins (Администраторы домена)	Read, Write, Create All Child Objects, Delete All Child Objects
Enterprise Admins (Администраторы предприятия)	Read, Write, Create All Child Objects, Delete All Child Objects
System (Система)	Read, Write, Create All Child Objects, Delete All Child Objects

Администраторы также являются аутентифицированными пользователями, т. е. имеют набор атрибутов Apply Group Policy. Если это нежелательно, у администраторов есть выбор.

- Удалить Authenticated Users из списка и добавить другую группу безопасности с атрибутом Apply Group Policy. Эта новая группа должна содержать всех пользователей, на которых будет влиять GPO.
- Запретить применение групповой политики для групп Domain Admins и Enterprise Admins и по возможности для группы Creator Owner. Это предотвратит применение GPO к членам этих групп. Помните: аннулирование разрешения всегда приоритетнее его предоставления. Следовательно, даже если пользователь — член другой группы, которой было дано разрешение Apply Group Policy, доступ ему по-прежнему будет запрещен.

Для редактирования GPO пользователь должен иметь доступ Read и Write к объекту. GPO нельзя открыть в режиме только для чтения. Иначе говоря, если Вы можете открыть

оснастку Group Policy, Вы можете редактировать объект Group Policy, появляющийся в левой панели. Более того, изменения вступают в силу сразу — отсутствует этап сохранения или активизации. Администратор может пожелать отсоединить GPO от любого сайта, домена или ОП при редактировании, а может пожелать оставить его присоединенным, но сделать неактивными узлы User и Computer.

Нельзя использовать группы безопасности для применения (или предотвращения применения) только некоторых параметров в объекте Group Policy, кроме случаев перенаправления папок и установки программ, которые имеют дополнительные **ACL,** установленные на уровне GPO для дальнейшего уточнения поведения, на основе членства в группах безопасности.

Редактировать GPO имеют право:

- Administrator (Администратор);
- Creator Owner (Создатель-владелец);
- пользователь с делегированным доступом к объекту Group Policy.

Можно изменять разрешения GPO, открыв окно свойств сайта, домена или **ОП.** содержащих GPO, и перейдя на вкладку Group Policy. Выберите GPO, щелкните кнопку Properties (Свойства) и перейдите на вкладку Security (рис. 7-15). Оттуда Вы можете изменять основные разрешения или щелкнуть кнопку Advanced (Дополнительно) для изменения дополнительных разрешений.

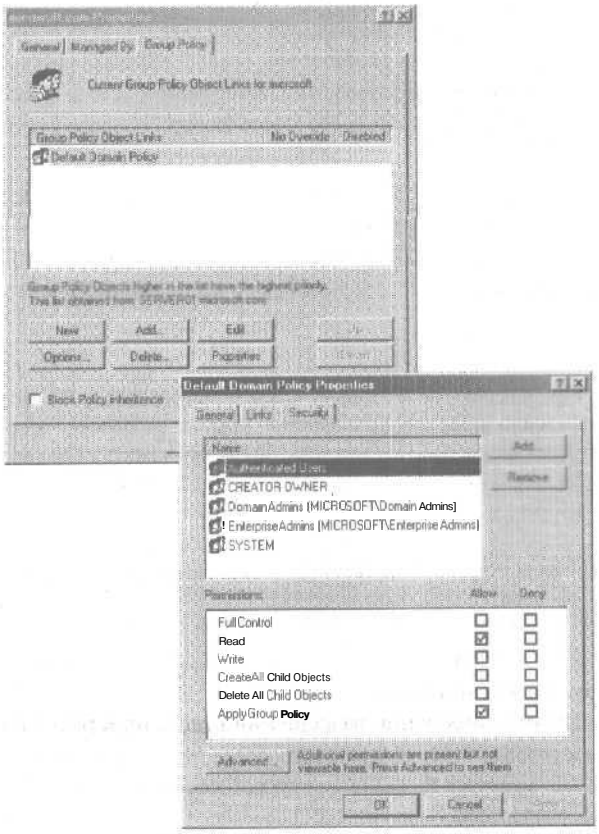


Рис. 7-15. Параметры безопасности домена microsoft.com

Порядок наследования

Как правило групповая политика передается от родительского к дочернему контейнеру. Групповая политика, назначенная родительскому контейнеру верхнего уровня, применяется ко всем нижележащим контейнерам, включая расположенные в них объекты пользователя и компьютера. Однако групповая политика дочернего контейнера, параметры которой заданы явным образом, имеет более высокий приоритет, чем родительского контейнера.

Если параметры политики родительского ОП не сконфигурированы, дочернее ОП их не наследует. Опущенные параметры политики наследуются как неактивные. Аналогично, если для родительского ОП политика сконфигурирована и та же самая политика не сконфигурирована для дочернего, последнее наследует политику родительского ОП.

Если родительская и дочерняя политики совместимы, дочернее ОП наследует политику родительского, и дочерняя настройка также применяется. Политики наследуются, пока они совместимы. Например, если родительская политика помешает определенную папку на рабочий стол, а для дочерних параметров нужна дополнительная папка, то пользователь видит обе папки.

Если политика родительского ОП конфликтует с политикой дочернего, политика первого не наследуется. Применяется настройка дочернего ОП.

Для конфигурирования наследования для доменов и ОП откройте окно свойств домена или ОП в оснастке Active Directory Users And Computers и выберите вкладку Group Policy. Кроме того, Вы можете конфигурировать наследование для узлов, используя оснастку Active Directory Sites And Services. Откройте окно свойств для определенного сайта и выберите вкладку Group Policy. Сконфигурировать наследование позволяют флажки Block Policy Inheritance (Блокировать наследование политики) и No Override (Не перекрывать).

Флажок Block Policy Inheritance

Заблокировать наследование на уровне домена или ОП позволяет флажок Block Policy Inheritance, расположенный на первой вкладке окна свойств GPO. Блокирование наследования политики неприменимо к политике сайта, так как он находится на вершине иерархии GPO. Если этот параметр выбран для GPO дочернего уровня, дочерний объект не наследует политик родительских GPO.

Флажок No Override

Заставляет все дочерние контейнеры наследовать родительские политики, даже если они конфликтуют с дочерними и для дочернего объекта установлен параметр Block Policy Inheritance. Этот флажок и тот, что описан ниже, можно увидеть, щелкнув кнопку Options (Параметры) в окне свойств GPO.

Флажок Disabled

Отключает GPO; при этом он по-прежнему ассоциируется с контейнером, в котором определен. Этот параметр обычно используют для изменения параметров в политике без влияния на пользователей. По завершении изменений сброс этого флажка применяет GPO ко всем пользователям, имеющим разрешение Apply Group Policy.

Удаление стандартной политики домена

По умолчанию Default Domain Policy GPO не может быть удален ни одним администратором. Это сделано для предотвращения случайного удаления этого GPO, содержащего важные для домена сведения. Если применять Default Domain Policy нет необходимости, например, из-за того, что политики были настроены в других GPO, пометьте флажки Disable Computer Configuration и Disable User Configuration в свойствах Default Domain Policy. Вы можете также пометить флажок Block Policy Inheritance для GPO ниже в иерархии, чтобы

политика домена по умолчанию не применялась. Эти параметры будут действовать, пока для родительского GPO не задан параметр No Override.

Поддержка для Windows 9x и Windows NT 4.0

Оснастка Group Policy не обеспечивает клиентскую поддержку для компьютеров с Windows 95/98/NT 4.0.

Поддержка клиентов Windows NT 4.0 обеспечивается полной поддержкой административных шаблонов в стиле Windows NT 4.0 (файлы .adm) и предоставлением файлов System Policy Editor для Windows NT 4.0 (Poledit.exe). Клиентами Windows 95/98 по-прежнему следует управлять, используя System Policy Editor для Windows 9x.

Для компьютеров с Windows 95/9S надо созданный в ОС клиентского компьютера файл Config.pol скопировать на сетевой ресурс, подключаемый при регистрации в домене. Клиенты Windows NT 4.0 используют файл Ntconfig.pol, который они считывают из сетевого ресурса. В сети Windows NT Server ресурс входа, именуемый Netlogon, находится в папке %systemroot%\System32\Repl\Import\Scripts. Сетевой ресурс входа для Windows 2000 находится в папке %systemroot%\ SYSVOL\Sysvol\<*имя_домена.com*>\Scripts и имеет общее имя Netlogon. Клиентские компьютеры Windows 9x/NT обращаются к этому ресурсу для доступа к соответствующему файлу .pol.

Об установке System Policy Editor см. справочную систему Windows 2000 Server. Редактор System Policy Editor включен в Windows 2000 Server, но не включен в Windows 2000 Professional. Пакет средств администрирования Windows 2000 (Adminpak.msi), куда входит System Policy Editor, поставляется на компакт-диске Windows 2000 Server для установки на компьютеры с Windows 2000 Professional. Для запуска редактора политики Windows NT в окне Run (Запуск программы) введите **poledit**.

Администрирование групповых политик

Настроив GPO и сконфигурировав консоль MMC, содержащую оснастку Group Policy для каждого из GPO, можно приступить к администрированию групповых политик.

Управление настройками программ

Для централизованного управления распространением ПО служит оснастка Group Policy. ПО может быть установлено, назначено, опубликовано, обновлено, исправлено и удалено для групп пользователей и компьютеров.

Перед использованием оснастки Group Policy для развертывания ПО Вы должны приобрести пакеты Microsoft Windows Installer (.msi) для приложений. Это можно сделать следующим образом.

- Поставщик или разработчик ПО может поставлять пакеты Windows Installer для своих приложений. Например, так делает Microsoft. Сторонние поставщики средств установки ПО обеспечат разработчиков инструментами создания пакетов Windows Installer для самостоятельного создания пакетов.
- Администратор может создать переупакованный пакет Windows Installer для приложения, используя инструменты переупаковки, предоставленные сторонними поставщиками.

Назначение и публикация приложений

Вы можете назначать приложения пользователям и компьютерам и публиковать приложения пользователям.

*Назначение **пользователям***

Пользователю, которому назначено приложение, предлагается установить его при следующем входе на рабочую станцию. Оповещение приложения следует за пользователем независимо от того, на каком компьютере он работает в настоящее время. Это приложение устанавливается, как только пользователь первый раз активизирует приложение на компьютере, выбрав его в меню Start (Пуск) или открыв связанный с ним документ.

***Назначение** компьютерам*

Приложение, назначенное компьютеру, предлагается пользователям и устанавливается, когда это безопасно — обычно при запуске компьютера, когда в нем нет конфликтующих процессов.

Публикация пользователям

Приложение, опубликованное пользователям, не появляется среди установленного на компьютерах ПО. Ни на рабочем столе, ни в меню Start ярлыков не видно, и в локальный реестр на компьютерах пользователей изменения не вносятся. Вместо этого опубликованные приложения хранят свои атрибуты оповещения в хранилище Active Directory. Затем информация, например имя приложения и файловые ассоциации, представляется пользователям в контейнере Active Directory. Впоследствии пользователь может установить приложение, выбрав Add/Remove Programs в Control Panel или щелкнув файл, связанный с приложением (например, .xls для Microsoft Excel).

Назначение и публикация приложений

Создайте обшую папку и скопируйте в нее файлы приложений и пакетные файлы (файлы .msi). Присвойте папке разрешения:

- Everyone=Read;
- Administrators=Full Control.

Чтобы назначить или опубликовать приложение, откройте оснастку Group Policy для соответствующего GPO и выберите подкаталог установки Software Settings\Software из узла Computer Configuration или User Configuration. В меню Action выберите команду New, затем — Package. Просмотрите созданный сетевой ресурс и выберите пакет, который хотите назначить. Откроется окно Deploy Application. Выберите метод развертывания.

Щелкните Assigned:Deployed To All Users At Logon или Published:Users Install Via Add/Remove Programs wizard и щелкните OK. На правой панели появится имя приложения, которое Вы хотите назначить или опубликовать, и его дополнительные свойства.

Приложения развертываются так:

Если приложение	в узле	оно появляется в
назначено	User Configuration	меню Start для всех пользователей в сайте, домене или ОП
	Computer Configuration	меню Start для всех компьютеров в сайте, домене или ОП
опубликовано	User Configuration	мастере Add/Remove Programs для всех пользователей в сайте, домене или ОП
	Computer Configuration	мастере Add/Remove Programs для всех компьютеров в сайте, домене или ОП

Управление сценариями

Групповая политика Windows 2000 позволяет достаточно гибко назначить сценарии. Вы можете назначить компьютерам сценарии включения и выключения, а пользователям - сценарии входа и выхода, выполняемые в процессе регистрации пользователя в системе или выхода из нее.

Windows 2000 выполняет сценарии следующим образом.

- Когда Вы назначаете несколько сценариев включения и выключения или входа и выхода пользователю или компьютеру, Windows 2000 выполняет сценарии сверху вниз. Вы можете определить порядок выполнения нескольких сценариев в окне свойств.
- При выключения компьютера Windows 2000 сначала выполняет сценарии выхода, а затем выключения. По умолчанию на выполнение сценариев отводится 2 минуты. Если для выполнения сценариев выхода и выключения требуется больше времени, измените значение времени в политике ПО.

Примечание Windows 2000 хранит сценарии для GPT в папке Scripts.

Оснастка Group Policy в Windows 2000 позволяет назначать как сценарии включения/выключения компьютерам, так и входа/выхода пользователям. Сценарии выполняются при возникновении определенного события через расширение Scripts (Startup/Shutdown) для компьютеров и расширение Scripts (Logon/Logoff) для пользователей.

Сценарии, которые можно использовать, включают командные файлы Windows NT (.bat или .cmd), VBScript (.vbs) или JScript (.js).

Для назначения сценариев дважды щелкните соответствующий значок сценария (Startup, Shutdown, Logon или Logoff), затем — кнопку Add и выберите нужный сценарий Затем введите для него параметры командной строки.

Использование нескольких сценариев

Пользователю/компьютеру может быть назначено несколько сценариев Logon/Logoff или Startup/Shutdown. Задать порядок выполнения в случае выбора нескольких сценариев позволяют кнопки Up и Down в окне свойств. Сценарии будут выполняться сверху вниз.

Кнопка Show Files

Щелкнув кнопку Show Files (Показать файлы), Вы откроете окно, отображающее содержимое папки сценариев. Это позволяет просматривать сценарии и связанные с ними файлы, существующие для данного GPO.

Управление параметрами безопасности

Политика безопасности покрывает различные области политики, административных прав и разрешений пользователей. В Windows 2000 определены два вида политики безопасности:

- домена;
- компьютера (известна также как локальная политика).

На компьютер, не включенный в домен Windows 2000, влияет только политика безопасности компьютера. К компьютеру — члену в домене Windows 2000 сначала применяется политика безопасности компьютера, а затем — политика безопасности домена.

Windows 2000 предоставляет инфраструктуру для определения и централизованного управления этими политиками безопасности и соблюдает их на всех компьютерах в домене. Инфраструктуру безопасности можно разделить на несколько конфигурируемых категорий.

- **Account Policies** позволяет конфигурировать параметры безопасности для политик паролей, блокировки и Kerberos в доменах Windows 2000,
- **Local Policies** позволяет конфигурировать параметры безопасности для полигики аудита и предоставления прав пользователям. Применяя локальную политику, Вы можете определить тех, кто имеет локальный или сетевой доступ к компьютеру, и способ аудита локальных событий.
- **Event Log** позволяет конфигурировать параметры безопасности для журналов Application, Security и System. Получить доступ к этим журналам можно через оснастку Event Viewer (Просмотр событий).
- **Restricted Groups** позволяет задать принадлежность к ограниченной группе и определить принадлежность ограниченной группы к другим группам. Эти параметры служат для усиления политики безопасности в отношении важных групп, например. Enterprise Administrators. Если к группе временно добавляется новый пользователь, при повторном применении политики он автоматически удаляется из группы Enterprise Administrators. По умолчанию политики применяются каждые 90 минут. Следовательно, временный пользователь будет иметь привилегии администратора предприятия не более 90 минут.
- **System Services** позволяет конфигурировать режим запуска и параметры безопасности (дескрипторы безопасности) для системных служб: сетевых, файлов и принтеров, телефонов и факсов, и т. д,
- **Registry** позволяет конфигурировать параметры безопасности для разделов реестра, включая контроль доступа, аудит и владение. Если задана безопасность разделов реестра, расширение Security Settings следует той же модели наследования, что применяется для всех древовидных иерархий Windows 2000 (например, хранилища Active Directory и NTFS). Microsoft рекомендует использовать наследование для определения безопасности только на объектах верхнего уровня и переопределять безопасность только для тех дочерних объектов, которым э го надо. В итоге заметно упрощается структура безопасности и сокращаются административные издержки, вызванные сложностью структуры управления.
- **File System** позволяет конфигурировать параметры безопасности для объектов файловой системы, включая управление доступом, аудит и владение.
- **Public Key Policies** позволяет конфигурировать агенты восстановления зашифрованных данных, политику автоматической выдачи сертификатов, доменные корни и доверенные центры сертификации.
- **IP Security Policies on Active Directory services** позволяет конфигурировать безопасность IP в сети.

Набор предопределенных шаблонов конфигурации безопасности хранится в папке %systemroot%\Security\Templates. Эти шаблоны можно использовать как основу для параметров безопасности и впоследствии отредактировать в соответствии с потребностями организации.

Конфигурации безопасности хранятся в виде INF-файлов в текстовом формате Security Descriptor Definition Language (SDDL) Когда конфигурация безопасности назначается или редактируется, обрабатывается файл конфигурации и изменения вносятся в сопоставленные компьютеры или учетные записи пользователей.

Управление административными шаблонами

Чтобы указать параметры реестра, которые можно изменить через оснастку Group Policy, применяется расширение Administrative Templates и файл административного шаблона

(.adm). Каждая политика перечисляет параметры политик, применяемые к выбранному сайту, домену или ОП.

Политики, перечисленные в Administrative Templates, представляют параметры групповой политики в реестре. Шаблоны Administrative Templates управляют поведением Windows 2000, компонентов ОС и приложений. Эти параметры записываются в разделы реестра HKEY_CURRENT_USER(HKCU) или HKEY_LOCAL_MACHINE (HKLM) соответственно.

Файл .adm является текстовым файлом в формате Unicode (поддержка формата Unicode для файлов .adm — новинка Windows 2000). Этот файл определяет иерархию категорий и подкатегорий, совместно определяющих отображение параметров, указывает на место в реестре, где должны быть сделаны изменения, определяет любые параметры или ограничения (в значениях) и в некоторых случаях определяет значение по умолчанию.

Вкладка Explain окна свойств каждой политики содержит описание параметров политики внутри файла .adm. На рис. 7.16 показана вкладка Explain для политики System.

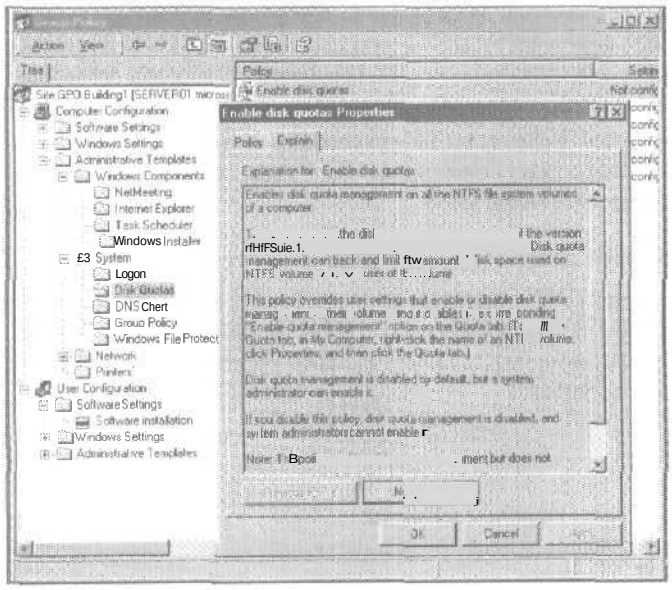


Рис. 7-16, Вкладка Explain (Объяснение) для свойства системы Enable Disk Quotas (Включить дисковые квоты)

Узлы Administrative Templates оснастки Group Policy могут быть дополнены пользовательскими файлами .adm.

Постоянные параметры реестра

Параметры реестра Windows NT 4.0 остаются в силе, пока они не отменяются явным образом. Настройки реестра Windows 2000, напротив, очищаются и перезаписываются после каждого изменения политики. Помните об этом при использовании политик, если Вы привыкли к поведению реестра Windows NT 4.0.

Управление перенаправлением папок

Расширение Folder Redirection позволяет перенаправлять любую из следующих специальных папок в профиле пользователя в новое место (например, сетевой ресурс):

- Application Data;
- Desktop (Рабочий стол);
- My Documents (Моидокументы);
- My Documents\My Pictures (Моидокументы\Мои рисунки);
- Start Menu (Главное меню),

Например, Вы могли бы перетравить пользовательскую папку My Documents на *\\сервер\ресурс*%username%.Это дает следующие преимущества.

- Обеспечение доступа к личным документам с любого компьютера в сети.
- Ускорениевхода/выхода из сети. В Windows NT 4.0 папка My Documents является частью перемещаемого профиля. Это значит, что папка My Documents и ее содержимое копируются между клиентским компьютером и сервером, когда пользователи входят/выходят из системы. Вынос папки My Documents за рамки профиля пользователя может значительно ускорить этот процесс.
- Хранение данных пользователя л сети (вместо локального компьютера). Данными в сети можно централизованно управлять и защищать их, применяя процедуры резервного копирования и доменные корни DFS.
- Предоставление пользователям доступа к папке My Documents в момент, когда они отсоединены от корпоративной сети, с помощью технологии автономных папок.

По умолчанию расширение Folder Redirection не включено в оснастку Group Policy. Для использования Folder Redirection нужно создать консоль MMC, содержащую оснастку Group Policy для каждого поддерживаемого GPO.

Упражнение 6: создание объекта групповой политики и настройка политики

Создайте для своего домена GPO с именем Domain Policy, затем из остнастки Group Policy измените параметры безопасности GPO, чтобы разрешить группе Domain Users (Пользователи домена) локально входить на контроллеры домена. Выполняйте упражнение на Server01.

► Задание 1: создайте GPO

Создайте GPO на уровне домена.

1. Войдите в домен как Administrator с паролем **password**.
2. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык Active Directory Users And Computers.

   Откроется остнаска Active Directory Users And Computers.
3. В дереве консоли щелкните microsoft.com, затем в меню Action выберите команду Properties.

   Откроется окно свойств microsoft com.
4. Перейдите на вкладку Group Policy (Групповая политика) и щелкните кнопку Add (Добавить).

   Откроется окно Add A Group Policy Object Link (Добавить ссылку на объект групповой политики).
5. Перейдите на вкладку АН (Все).

   В списке имеется Default Domain Policy. Вы могли бы использовать этот GPO и изменять его по своему желанию, но сейчас создайте для домена новый GPO.
6. Щелкните среднюю из трех имеющихся на панели инструментов кнопок.

   В перечне GPO появится New Group Policy Object (Новый объект групповой политики).

7. Назовите новый GPO **Domain Policy** и щелкните кнопку OK.
   В столбце Group Policy Object Links (ссылки на объекты групповой политики) появится объект Domain Policy.
8. Щелкните кнопку OK, чтобы закрыть окно свойств политики.
9. Оставьте оснастку Active Directory Users And Computers открытой.

► **Задание 2: измените параметры безопасности**

С помощью редактора Group Policy измените параметры безопасности, чтобы разрешить группе Domain Users локально входить на Server01.

1. В дереве консоли раскройте microsoft.com.
2. Щелкните контейнер Domain Controllers.
3. В меню Action (Действие) выберите команду Properties (Свойства).
   Откроется окно Domain Controllers Properties.
4. Перейдите на вкладку Group Policy.
   Убедитесь, что в списке Group Policy Object Links выбрана строка Default Domain Controllers Policy, и шелкните кнопку Edit.
5. Откроется оснастка Group Policy, отображающая дерево консоли Default Domain Controller Policy.
6. Проверьте, что узел Computer Configuration в дереве консоли раскрыт.
7. Раскройте в узле Computer Configuration узел Windows Settings\Security Settings\Local Policies.
8. В объекте Local Policies щелкните User Right Assignment.
   На правой панели появится список атрибутов User Right Assignment.
9. На правой панели дважды щелкните Log On Locally.
   Откроется окно Log On Locally. Заметьте: этот параметр политики назначен нескольким пользователям и группам.
10. Щелкните кнопку Add.
    Откроется окно Add User Or Group.
11. Щелкните кнопку Browse.
    Откроется окно Select Users Or Groups,
12. В списке Name выберите Domain Users (Пользователи домена), щелкните кнопку Add, затем — OK.

Совет Если у Вас возникли затруднения при поиске группы Domain Users, просто введите **Domain Users,** и Windows сама найдет эту группу.

---

13. Еще раз щелкните кнопку OK.
    Группа Domain Users появится в списке пользователей и групп с правом локального входа.
14. Щелкните кнопку OK и закройте оснастку Group Policy.
15. Щелкните кнопку OK, чтобы закрыть окно Domain Controllers Properties.
16. Оставьте открытой оснастку Active Directory Users And Computers — она понадобится в следующим упражнении.
    Теперь все пользователи домена могут входить на ServerOl локально.

Упражнение 7: изменение политик ПО

Создайте и затем измените групповую политику ОП Sales, удалив из меню Start пункты Search (Найти) и Run (Выполнить). Вы также отключите политику Lock Workstation и просмотрите результаты этих изменений политики ПО. Наконец, Вы сделаете так, чтобы политика ОП Sales не перекрывала групповую политику его родительского контейнера, домена. Выполняйте упражнение на Server01.

► Задание 1: измените политики ПО

Создайте и измените политики ПО для ОП Sales, созданного в главе 6.

1. В оснастке Active Directory Users And Computers раскройте узел microsoft.com.
2. В дереве консоли шелкните Sales, затем в меню Action выберите команду Properties.
   Откроется окно Sales Properties (Свойства: Sales).
3. Перейдите на вкладку Group Policy (Групповая политика).
4. Щелкните кнопку Add.
   Откроется окно Add A Group Policy Object Link.
5. Перейдите на вкладку All и щелкните среднюю из трех кнопок на панели инструментов.
   В списке Group Policy Objects Associated With This Container появится новый GPO.
6. Назовите новый GPO SalesSoftware и щелкните кнопку OK.
   Вернитесь на вкладку Group Policy окна свойства ОП Sales.
7. Выделите SalesSoftware и щелкните кнопку Edit (Изменить).
   Откроется оснастка Group Policy.
8. Найдите и раскройте шаблоны Administrative в узле User Configuration.
9. В дереве консоли шелкните Start Menu & Task Bar.
   На правой панели появятся политики, доступные для этой категории.
10. На правой панели дважды щелкните Remove Search Menu From Start Menu.
    Откроется окно свойств этой политики.
11. Перейдите на вкладку Explain, чтобы прочитать описание этой политики.
12. Перейдите на вкладку Policy и шелкните переключатель Enabled.
13. Щелкните кнопку OK.
14. Повторите пп. 10-13 для активизации политики Remove Run Menu From Start Menu.
15. В дереве консоли дважды щелкните System, затем Logon/Logoff.
    На правой панели появятся политики, доступные для этой категории.
16. На правой панели активизируйте политику Disable Lock Computer.
17. Закройте оснастку Group Policy, затем закройте окно Sales Properties.
18. Закройте оснастку Active Directory Users And Computers.

► Задание 2: протестируйте политики ПО

Изучите действие политик ПО, созданных на предыдущем этапе.

Внимашив! После выполнения упражнений этой главы и главы 6 в ОП Sales должны находиться учетные записи пользователей Jane Doe и John Smith.

---

1. Завершите на ServerOl сеанс администратора.
2. Нажмите клавиши Ctrl+Alt+Delete.
3. Откроется окно Windows Security.
   Кнопка Shutdown недоступна. Это контролируется политикой Shutdown Without Logon. Windows 2000 Server не делает эту кнопку доступной по умолчанию.

4. Зарегистрируйтесь на Server01 как Jane_Doe с паролем student.
5. Раскройте меню Start.

   Заметьте: пункты Search и Run в меню Start не отображаются.

▶ **Задание 3: предотвратите перекрытие групповой политики**

Вы помешаете ОП Sales перекрыть групповую политику его родительского контейнера.

1. Зарегистрируйтесь как Administrator с паролем **password.**
2. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык Active Directory Users And Computers.

   Откроется оснастка Active Directory Users And Computers.
3. Раскройте узел microsoft.com.
4. Щелкните Sales, затем выберите в меню Action команду Properties.

   Откроется окно Sales Properties.
5. Перейдите на вкладку Group Policy.
6. Проверьте, что в списке Group Policy Objects Link выбрана строка SalesSoftware, и щелкните кнопку Options.
7. Пометьте флажок No Override: Prevents Other Group Policy Objects From Overriding Policy Set In This One, затем щелкните кнопку OK.
8. Еще раз щелкните кнопку OK и закройте оснастку Active Directory Users And Computers.

Резюме

Групповая политика — это набор параметров конфигурации, применяемых к одному или нескольким объектам в хранилище Active Directory. Политики позволяют управлять рабочей средой пользователей в сайте, домене или ОП. Существует много видов групповых политик, включая параметры ПО и безопасности, административные шаблоны и перенаправление папок, Структура групповой политики состоит из объектов групповой политики, контейнеров и шаблонов. Перед созданием групповой политики надо создать объекты GPO. Из них можно редактировать групповую политику, используя оснастку Group Policy, или управлять разрешениями, применяя оснастку Active Directory Users And Computers. Администрирование групповых политик включает в себя управление параметрами ПО, сценариями, параметрами безопасности, административными шаблонами и перенаправлением папок.

Закрепление материала

? J Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Можно ли добавить к стандартным консолям Windows 2000 Server оснастки? Почему?

2. Пользователи жалуются на окно, появляющееся каждый раз, когда они входят в систему. В меню Startup (Автозагрузка) нет ярлыков. После закрытия окна, выхода из системы и перезагрузки компьютера окно по-прежнему появляется при входе в систему. Какова наиболее вероятная причина этой проблемы и как ее устранить?

3. В каких случаях использовать группы безопасности вместо групп распространения?

4. Каковы последствия изменения режима домена со смешанного на основной?

5. В каком порядке по умолчанию реализована групповая политика в иерархии хранилища Active Directory?

6. Что такое GPO, GPC и GPT?

ГЛАВА 8

Управление печатью

В этой главе

В этой главе рассказано об установке и настройке сетевых принтеров. **Вы** также узнаете о печати с помощью Active Directory и способах подключения к сетевым принтерам. Кроме того, здесь описано устранение типичных проблем, возникающих при настройке сетевых принтеров.

Прежде всего

Для изучения материалов этой главы необходимо:

- установить Microsoft Windows 2000 Server;
- установить Active Directory;
- выполнить все упражнения из предыдущих глав.

Примечание Для выполнения упражнений этой главы принтер не требуется.

Занятие 1. Основы печати в Windows 2000

Microsoft Windows 2000 Server поддерживает сетевую печать. Приложения, выполняемые на разных платформах, направляют задания на принтеры, подключенные к серверу печати Windows 2000, напрямую к сети — через внутренние или внешние сетевые платы — или к другому серверу. Сервер печати на базе Windows 2000 Server позволяет печатать на любом подключенном к сети компьютере с любой ОС, поддерживаемой Windows 2000. На этом занятии Вы познакомитесь с терминологией и узнаете основные принципы создания среды сетевой печати. Мы обсудим также вопросы, связанные с локальной и удаленной печатью и с устройствами печати, подключенными к сети или к компьютеру.

Изучив материал этого занятия, Вы сможете:

- ✓ объяснить термины печати в Windows 2000;
- ✓ перечислить основные требования к среде сетевой печати;
- ✓ описать сценарии локальной и удаленной печати для устройств печати, подключенных к сети или к компьютеру.

Продолжительность занятия — около 35 минут.

Терминология

Терминология печати в Windows 2000 позволяет понять принципы взаимодействия компонентов (рис. 8-1).

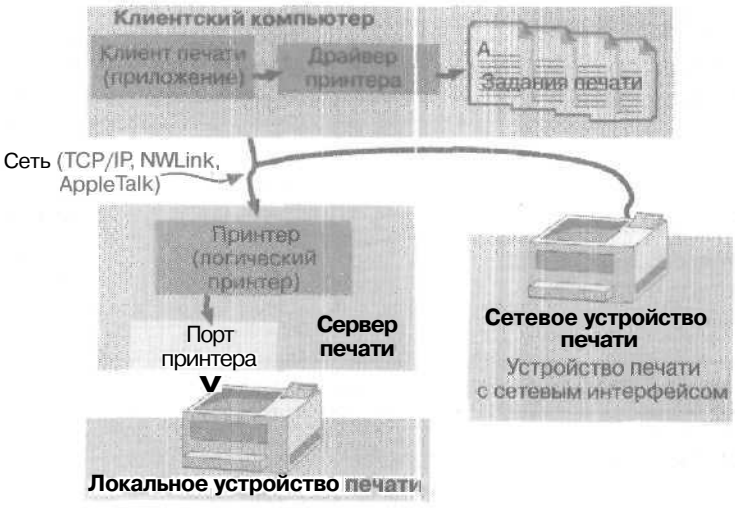


Рис. 8-1. Терминология печати

Если Вы только начинаете работу с Windows 2000, то используемая здесь терминология Вам может показаться непривычной (хотя в сравнении с Microsoft Windows NT Server она не претерпела существенных изменений). Основные понятия, используемые при печати в Windows 2000, таковы.

- **Принтер.** Программный интерфейс между ОС и устройством печати. Он определяет, куда и когда передать документ, чтобы он попал на устройство печати (локальный порт, порт для сетевого подключения или файл), а также обеспечивает обработку процесса

печати. Для соединения с принтером пользователь применяет имя принтера, указывающее на одно или несколько устройств печати.

- **Устройство печати.** Аппаратное устройство, печатающее документы. Windows 2000 поддерживает следующие типы устройств печати.
  - *Локальное устройство печати* (local print device) подключается к физическому порту сервера печати; соединяется с компьютером через локальный интерфейс, например параллельный или последовательный RS-232/422/IRDA, USB или порт **SCSI.**
  - *Сетевое устройство печати* (network print device) подключается к серверу печати через сеть, а не через физический порт. Сетевые устройства печати, или *устройства печати с сетевым интерфейсом* (network-interface print devices), должны обладать собственными сетевыми интерфейсными платами и иметь собственный сетевой адрес, либо подключаться к внешней сетевой плате. Сетевой принтер является узлом в сети, поэтому задания на печать посылаются на него через сетевую плату (обычно встроенную).
- **Сервер печати.** Компьютер, с которым ассоциированы принтеры, связанные с локальными и сетевыми устройствами печати. Получает и обрабатывает документы, поступающие с клиентских компьютеров. Позволяет устанавливать и эффективно совместно использовать сетевые принтеры на серверах печати.
- **Драйвер принтера.** Так называется файл, позволяющий Windows 2000 преобразовать команды печати в команды языка конкретного принтера, например PostScript. Эти преобразованные команды и заставляют устройство печатать документ. У каждого устройства печати свой драйвер.

Программные и аппаратные требования сетевой печати

- Минимум один компьютер, функционирующий как сервер печати. Если такому серверу приходится управлять большим числом интенсивно используемых принтеров, рекомендуется внедрить выделенный сервер печати. Этот компьютер может управляться следующими ОС:
  - Windows 2000 Server — способна обрабатывать большое количество подключений и взаимодействует с клиентскими компьютерами под управлением клиентских перенаправителей и служб доступа к принтерам MS-DOS, Windows, Macintosh, UNIX и NetWare;
  - Windows 2000 Professional — способна обрабатывать не более 10 параллельных подключений с другими компьютерами, осуществляющими доступ к файлам и принтерам; работает с клиентами MS-DOS, Windows и UNIX, но не поддерживает клиенты Macintosh и NetWare.
- Достаточный для обработки документов объем ОЗУ. Если сервер печати управляет большим числом принтеров или обрабатывает крупные документы, ему может потребоваться дополнительная память, иначе скорость печати снизится.
- Достаточный размер дискового пространства на сервере печати, чтобы посланные на сервер печати данные могли быть временно (до отправки на устройство печати) сохранены на диске. Это особенно важно, когда на сервер посылается либо много документов, либо документы большого размера. Например, если 10 пользователей пошлют одновременно на печать большие документы, то серверу печати потребуется разместить на жестком диске все файлы заданий печати и сохранять их там до посылки на устройство печати. Если на жестком диске не хватит места, пользователи получат сообщение об ошибке и не смогут напечатать документы.

Примечание Размер файлов заданий печати в очереди может значительно превышать размер печатаемого документа из-за предварительной обработки задания печати драйвером принтера.

Рекомендации по созданию сетевой среды печати

Перед настройкой сетевой печати подумайте, как оптимальным образом удовлетворить потребности пользователей.

Рекомендация	Объяснение
Определите требования пользователей к печати	Выясните, скольким пользователям необходимо распечатывать документы, и оцените объем печати. Например, 15 сотрудникам отдела выписки счетов, постоянно печатающим счета, потребуется больше принтеров, устройств печати и, возможно, серверов печати, чем 15 разработчикам ПО, выполняющим всю работу в электронном виде.
Определите требования организации к печати	Определите потребности организации в печати (количество и типы устройств печати, нагрузку на каждый принтер). Не используйте для сетевой печати персональные устройства печати
Определите количество серверов печати	Определите количество серверов печати, необходимое для управления имеющимися в Вашей сети принтерами.
Определите, где расположить устройства	Определите оптимальное расположение устройств печати. В маршрутизированных печати сетях постарайтесь разместить серверы печати и управляемые ими устройства печати в одной подсети с использующими их клиентскими компьютерами. Помимо всего прочего, это позволит пользователям быстро получать напечатанные документы.

Конфигурации печати

Windows 2000 позволяет создавать несколько различных конфигураций клиентов, серверов и устройств печати. Конфигурация определяется удаленностью устройства печати. Доступ к удаленному устройству печати осуществляется через сервер печати. Второй фактор, определяющий конфигурацию, — способ подключения устройства печати: оно может быть подключено к сети либо прямо к компьютеру.

Ниже показаны 4 основных конфигурации печати. Тонкие линии обозначают физические соединения — сетевые или параллельные кабели, а стрелки — логические потоки данных печати.

Рис. 8-2. Конфигурация с неудаленным локальным устройством печати

Простейшая конфигурация — с неудаленным локальным устройством печати (рис. 8-2). Устройство печати подключено к параллельному порту компьютера, на котором выполняется приложение. На этом же компьютере находится и драйвер принтера, и очередь заданий на печать. Данные пересылаются на устройство печати напрямую.

Небольшая группа компьютеров, совместно использующих сетевое устройство печати, является одноранговой сетью, так как все компьютеры имеют равноправный доступ к устройству печати; централизованного управления печатью и безопасностью нет (рис. 8-3). Каждый компьютер формирует свою очередь печати и не видит очередей печати на других компьютерах. Если произойдет непредвиденная остановка печати, сообщение об ошибке получат не все клиенты. Такой вариант приемлем для небольших организаций, где пользователи постоянно контактируют друг с другом, однако при увеличении трафика отсутствие управления скажется негативно. Соперничество компьютеров за ресурсы устройства печати может привести к его отказу.

Рис. 8-3. Конфигурация с неудаленным сетевым устройством печати

На рис. 8-4 изображена конфигурация с центральным сервером печати. Клиенты осуществляют совместный доступ к принтеру через сервер печати, к которому локально подсоединено устройство печати. Очередь печати находится на сервере и видима каждому клиенту.

Рис. 8-4. Конфигурация с удаленным локальным устройством печати

Процесс печати в этом случае контролирует администратор сервера, который разрабатывает и внедряет систему безопасности для сети, следит за работой ПО принтера и затру-

жает его клиентам, когда они соединяются с принтером. Если на сервере печати установлены более свежие драйверы, то при подключении клиента к сетевому принтеру клиентские драйверы обновляются автоматически.

В этой конфигурации клиенты могут также подключаться к другим устройствам печати, а к серверу печати зачастую подсоединено несколько таких устройств. Впрочем, число устройств печати ограничено количеством параллельных портов на сервере печати.

На рис. 8-5 показано несколько клиентов, совместно использующих устройство печати в домене Windows 2000 Server. Устройство печати соединено с сервером печати через сеть, что позволяет одному серверу печати управлять несколькими устройствами печати.

Установка и предоставление общего доступа к принтеру производится на сервере печати с помощью мастера Add Printer. Ссылка на него находится в папке Printers. Чтобы открыть ее, раскройте меню Start\Settings и щелкните ярлык Printers. Независимо от расположения устройств печати ПО для принтера всегда должно находиться на сервере печати. Если устройство печати подключено к серверу печати, мастер Add Printer (Мастер установки принтера), обнаружив его, пытается сконфигурировать ПО принтера. В противном случае в процессе настройки ПО принтера надо создать для устройства печати порт. Мастер Add Printer также применяется для соединения с удаленными устройствами печати. При этом помните следующее.

- *Установка принтера* (creating a printer) подразумевает установку устройства печати на сервер печати либо в сети, а также настройку управляющего ПО на сервере печати. Для установки принтера запустите мастер Add Printer, щелкните переключатель Local Printer (Локальный принтер), затем введите имя принтера, установите драйвер принтера и укажите порт.
- *Подключение к принтеру* (connecting to a printer) подразумевает подключение к ресурсу компьютера, на котором установлен принтер. Для подключения к принтеру запустите мастер Add Printer и щелкните переключатель Network Printer (Сетевой принтер). Если на сервере печати есть драйвер принтера для клиентской платформы, то устанавливать его на компьютер клиента не нужно — Windows 2000 загрузит его автоматически. Это касается драйверов для Windows 9x и всех версий Windows NT. В противном случае Вас попросят установить ПО для принтера.

Рис. 8-5, Конфигурация с двумя удаленными сетевыми устройствами печати

Резюме

Принтер — это программный интерфейс между ОС и устройством печати. Устройство печати — это аппаратное средство, *печатающее* документы. Сервер печати — это компьютер, на котором располагаются принтеры, связанные с локальными и сетевыми устройствами печати. Драйвер принтера — это один или несколько файлов с информацией, используемой Windows 2000 для преобразования команд печати в команды языка конкретного принтера. Вы также должны знать требования для сетевой печати: наличие минимум одного компьютера, способного функционировать в качестве сервера печати, достаточный объем оперативной памяти и дискового пространства. Вы также должны уметь определять потребности Ваших пользователей и организации в печати, нужное количество серверов печати и уметь оптимально располагать устройства печати. В Windows 2000 предусмотрено несколько конфигураций клиентов, серверов и устройств печати. Конфигурация определяется тем, является ли устройство печати локальным или удаленным, а также подключено ли оно к сети или прямо к компьютеру.

Занятие 2. Установка сетевого принтера

Совместный доступ к принтеру позволяет нескольким пользователям печатать на нем документы. Можно установить принтер для устройства печати, подключенного к серверу печати напрямую либо по сети. В крупных организациях принтеры обычно ссылаются на сетевые устройства печати.

Изучив материал этого занятия, Вы сможете:

- ✓ определить условия для установки сетевого принтера и сетевых ресурсов печати;
- ✓ установить принтер для локального или сетевого устройства печати и предоставить доступ к нему;
- ✓ предоставить доступ к существующему принтеру.

Продолжительность занятия — около 35 минут.

Установка локального принтера

Принтеры для локального и сетевогс устройств печати устанавливаются практически одинаково. Для установки локального устройства печати на сервере печати запустите мастер Add Printer (Установка принтера) и з окне Local or Network printer (Локальный или сетевой принтер) щелкните переключатель Local Printer (Локальный принтер) (рис. 8-6).

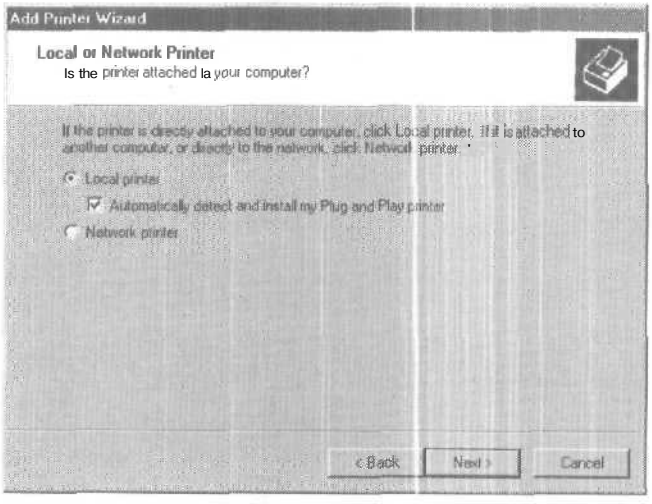


Рис. 8-6. Окно Local Or Network Printer (Локальный или сетевой принтер) мастера установки принтера

Мастер проведет Вас по этапам установки принтера для устройства печати, подключенного к серверу печати. Количество локальных устройств печати, которые можно подключить к серверу печати через физические порты, зависит от конфигурации аппаратуры.

Установка сетевого принтера

В крупных организациях большинство устройств печати являются сетевыми, так как они не обязательно должны находиться около сервера печати, а кроме того, по сетевым соединениям данные передаются быстрее, чем по кабелям принтера.

Принтер для сетевого устройства печати устанавливается с помощью мастера Add Printer. При этом в отличие от установки принтера для локального устройства печати, устанавливая сетевой принтер, надо указать информацию о дополнительном порте и сетевом протоколе.

Протоколом по умолчанию в Windows 2000 является TCP/IP. Его использует большинство сетевых устройств печати. Для TCP/IP сведения о дополнительном порте указываются с помощью мастера Add Standard TCP/IP Printer Port, вызываемого из мастера Add Printer. Подробнее об установке в Вашей сети принтера, использующего TCP/IP, см. справочную систему Windows.

Совместное использование принтера

Предоставляя общий доступ к принтеру, руководствуйтесь следующими правилами:

- присвойте принтеру сетевое имя — оно отображается в папке My Network Places (Мое сетевое окружение); имя должно быть содержательным, чтобы пользователям было легко найти нужный принтер;
- допускается установка драйверов принтера для Windows 9x, всех версий Windows NT и Windows 2000;
- Вы вправе опубликовать принтер в Active Directory, чтобы пользователи могли найти его со своего рабочего места.

Для предоставления доступа к имеющемуся принтеру откройте окно Printers (Принтеры), затем — диалоговое окно свойств соответствующего принтера и перейдите на вкладку Sharing (Доступ) (рис. 8-7).

После предоставления доступа к принтеру под значком принтера появится изображение руки — это значит, что к принтеру разрешен совместный доступ.

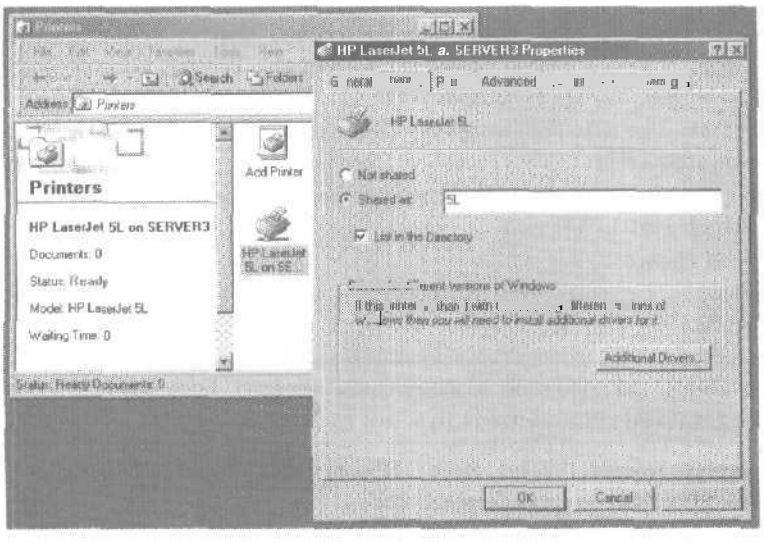


Рис. 8-7. Вкладка Sharing (Доступ) диалогового окна свойств принтера

Упражнение: установка принтера, настройка доступа к нему и настройка отложенной печати

С помощью мастера Add Printer (Установка принтера) установите на компьютер локальный принтер и откройте к нему совместный доступ. Для выполнения этого

упражнения устройство печати не требуется, поскольку взаимодействие с принтером будет осуществляться в автономном режиме, дабы избежать возникновения сообщений об ошибках в следующих упражнениях. Выполняйте это упражнение на Server01.

► **Задание 1: установите локальный принтер и настройте доступ к нему**

1. Войдите в домен как Administrator с паролем **password.**
2. В меню Start\Settings (Пуск\Настройка) щелкните ярлык Printers (Принтеры).

   Откроется окно Printers (Принтеры) со значком Fax. Служба факсов устанавливается при обычной установке Windows 2000 Server.
3. Дважды щелкните значок Add Printer (Установка принтера).

   Откроется окно мастера установки принтера.
4. Щелкните кнопку Next (Далее).

   В открывшемся окне Local Or Network Printer (Локальный или сетевой принтер) надо выбрать расположение принтера Так как Вы устанавливаете принтер на собственном компьютере, сделайте его локальным.
5. Убедитесь, что выбран переключатель Local Printer (Локальный принтер), сбросьте флажок Automatically Detect And Install My Plug And Play Printer (Автоматическое определение и установка принтера Plug and Play) и щелкните кнопку Next (Далее).

   Откроется окно Select The Printer Port (Выберите порт принтера).
6. Щелкните переключатель Create A New Port (Создать новый порт).

   Станет доступным раскрывающийся список Type (Тип порта),
7. Щелкните стрелку справа от списка Type (Тип порта).

   Предлагаются варианты Local Port и Standard TCP/IP Port.

   Локальный порт доступен всегда. Доступность других портов зависит от установленных сетевых протоколов. В нашем случае установлен протокол TCP/IP, поэтому имеется доступ к порту, основанному на этом протоколе.
8. Щелкните переключатель Use The Following Port (Использовать имеющийся порт) и убедитесь, что выбран порт LPT1.

   В этом упражнении предполагается, что устройство печати подключено к Вашему компьютеру напрямую через порт LPT1.
9. Щелкните кнопку Next (Далее).

   Мастер предложит ввести сведения об изготовителе и модели принтера. Выберите принтер HP LaserJet 5Si.

Совет Принтеры в списке расположены в алфавитном порядке. Если Вы не можете найти имя принтера, убедитесь, чго смотрите нужный раздел.

---

10. В списке Manufacturers (Изготовители) щелкните HP, а в списке Printers (Принтеры) — HP LaserJet 5Si. Затем щелкните кнопку Next (Далее).

    Откроется окно Name Your Printer (Назовите Ваш принтер). В поле Printer Name (Имя принтера) по умолчанию задано имя HP LaserJet 5Si — не будем его менять.
11. Убедитесь, что для параметра Do You Want Your Windows-Based Programs To Use This Printer As The Default Printer? (Использовать этот принтер по умолчанию в среде Windows?) выбран вариант Yes (Да).
12. Щелкните кнопку Next (Далее).

    Откроется окно Printer Sharing (Использование общих принтеров).

13. Убедитесь, что выбран переключатель Share As (Общий доступ).

    Вы можете присвоить альтернативное имя общему принтеру, которое используется для его идентификации в сети. Имя должно соответствовать правилам именования и может не совпадать с локальным именем принтера. Первоначально введенное имя принтера отображается рядом со значком принтера в системной папке Printers и в Active Directory. Имя общего принтера должно быть кратким для совместимости с другими ОС, например Windows 3.x.

14. В текстовом поле Share As (Общий доступ) введите **Printer1** и щелкните кнопку Next (Далее).

    Откроется окно Location And Comment (Размещение и комментарий).

Примечание Значения, введенные Вами в поля Location (Размещение) и Comment (Комментарий), отображаются Windows 2000 при поиске принтера в хранилище Active Directory. Вводить значения в эти поля необязательно, однако эта информация облегчит поиск принтера.

---

15. В текстовом поле Location (Размещение) наберите **Building 520, Floor 18, Office 1831,** а в Comment (Комментарий) — **Black and White Output Laser Printer — High Volume** и затем щелкните кнопку Next (Далее).

    Откроется окно Print Test Page (Напечатать пробную страницу).

    Печать пробной страницы помогает удостовериться, что принтер установлен корректно. Вы также вправе установить дополнительные драйверы для других версий Microsoft Windows.

16. Выберите No (Нет) и щелкните кнопку Next (Далее).

    Откроется окно Completing The Add Printer Wizard (Завершение работы мастера установки принтеров) со сводкой выбранных параметров.

17. Щелкните кнопку Finish (Готово).

    При необходимости Windows 2000 попросит указать местоположение дистрибутивных файлов Windows 2000 Server.

18. Если появился такой запрос, вставьте установочный CD-ROM с Windows 2000 Server и подождите около 10 секунд. В противном случае обратитесь к информации, изложенной после п. 20.
19. Если откроется окно Windows 20QO CD-ROM, закройте его.
20. Щелкните OK, чтобы закрыть диалоговое окно Insert Disk (Вставка диска).

    Windows 2000 скопирует файлы принтера, и значок для принтера HP LaserJet 5Si появится в окне Printers (Принтеры).

    Заметьте: под значком принтера изображена рука — это значит, что к принтеру разрешен совместный доступ. Галочка рядом с принтером означает, что принтер используется сервером печати по умолчанию.

21. Не закрывайте окно Printers (Принтеры) — оно понадобится Вам в следующем упражнении.

► Задание 2: переводите принтер в автономный режим и распечатайте пробный документ

Переведите созданный Вами принтер в автономный режим (режим отложенной печати). При отложенной печати посланные на принтер документы сохраняются на жестком диске компьютера, пока устройство печати не станет доступным. Перевод принтера в автономный режим позволит избежать возникновения сообщений об ошибках в последующих уп-

ражнениях. (В противном случае Windows 2000 выдавало бы сообщение об ошибке при каждой попытке отправить документ на устройство печати, не подключенное к компьютеру.)

1. В окне Printers (Принтеры) щелкните значок HP LaserJet 5Si.
2. Раскройте меню File (Файл) и выберите Use Printer Offline (Отложенная печать).
   При этом изменился значок принтера, а на левой панели окна Printers (Принтеры) — информация о статусе: Use Printer Offline (Отложенная печать).
3. В окне Printers дважды щелкните значок HP LaserJet 5Si.
   Обратите внимание: список посланных на печать документов пуст.
4. Раскройте меню Start\Programs\Accessories (Пуск\Программы\Стандартные) и щелкните ярлык Notepad (Блокнот).
5. В текстовом редакторе наберите любой текст.
6. Расположите окна текстового редактора и HP LaserJet 5Si так, чтобы можно было видеть содержимое обоих окон.

Совет Для этого щелкните правой кнопкой панель задач и выберите в контекстном меню команду Tile Windows Horizontally (Окна слева направо).

---

7. В окне программы Notepad раскройте меню File (Файл) и выберите команду Print (Печать).
   Открывшееся диалоговое окно Print (Печать) предлагает выбрать принтер и параметры печати. Вы увидите информацию о местоположении принтера и комментарии, которые Вы ввели при его создании. Там также показано, что принтер находится в автономном режиме. Для поиска принтера в хранилище Active Directory щелкните кнопку Find Printer (Найти принтер).

   Заметьте: в качестве принтера выбран HP LaserJet 5Si. Этот принтер используется сервером печати по умолчанию, поэтому он выбирается автоматически.
8. Щелкните кнопку Print (Печать).
   Notepad сообщит, что документ печатается на Вашем компьютере. Сообщение быстро исчезает с экрана, и на мощном компьютере Вы его даже не заметите.

   В окне HP LaserJet 5Si Вы увидите, что документ ожидает отправления на устройство печати. Документ сохраняется в очереди, так как включена отложенная печать. Иначе он был бы послан на устройство печати сразу.
9. Закройте программу Notepad, щелкнув No (Нет) при запросе на сохранение Вашего документа.
10. В окне HP LaserJet 5Si выберите посланный Вами на печать документ, а затем в меню Printer (Принтер) щелкните команду Cancel All Documents (Очистить очередь печати).
11. В окне подтверждения Ваших намерений щелкните кнопку Yes.
    Документ будет удален из очереди печати.
12. Закройте окно HP LaserJet 5Si, а затем — окно Printers.

Резюме

Принтеры для локального и сетевого устройств печати устанавливаются практически одинаково — *с* помощью мастера Add Printer (Установка принтера) на сервере печати, который проводит через все этапы установки принтера. По умолчанию сетевым протоколом в Windows 2000 является TCP/IP. Он используется большинством сетевых устройств печати. Если требования к печати в Вашей сети возросли и у Вас есть подключенный локально свободный принтер, Вы можете предоставить к нему общий доступ.

Занятие 3. Управление сетевыми принтерами

Вы узнаете об установке и управлении сетевыми принтерами. Круг обсуждаемых здесь вопросов охватывает управление принтерами и документами, использование обозревателя Web для управления принтерами, настройку пула и приоритета принтера, а также устранение типичных неполадок печати.

Изучив материал этого занятия, Вы сможете:

- ✓ осуществлять доступ к принтерам и назначать для них разрешения;
- ✓ управлять принтерами и документами;
- ✓ использовать обозреватель Web для управления принтерами;
- ✓ настраивать пул принтера;
- ✓ назначать принтерам приоритет.

Продолжительность занятия — около 90 минут.

Управление доступом к принтерам

Администрирование принтеров осуществляется через окно Printers (Принтеры), открываемое из меню Start (Пуск), либо с помощью функции поиска оснастки Active Directory Users And Computers (Active Directory — пользователи и компьютеры). Окно Printers позволяет выполнять все административные задачи, в то время как возможности оснастки Active Directory Users And Computers ограничены: например, отсюда нельзя перевести принтер в автономный режим.

В Microsoft Windows 2000 работа с принтерами строится на основе разрешений. Разрешения предоставляются через вкладку Security (Безопасность) диалогового окна свойств принтера и регулируют доступ пользователей к принтеру (рис. 8-8). Вы также можете предоставить разрешение управлять принтером на одном из двух уровней: принтеров и документов.

В целях защиты Вам может понадобиться ограничить доступ к принтерам. Разрешения также позволяют дать право на управление определенными принтерами пользователям, которые не являются администраторами. В Windows 2000 три уровня разрешений: Print (Печать), Manage Documents (Управление документами) и Manage Printers (Управление принтерами) (окно Permissions на рис. 8-8).

Разрешения можно как предоставлять, так и отменять. Как и в случае групповой политики или разрешений **NTFS,** приоритет всегда имеют отмененные разрешения. Например, если Вы выберете системную группу Everyone (Все), показанную на рис. 8-8, и пометите флажок Deny (Запретить) напротив Manage Documents (Управление документами), управлять документами не сможет никто, даже если Вы ранее предоставили такое разрешение какому-либо пользователю или группе, поскольку все учетные записи пользователей являются членами системной группы Everyone.

По умолчанию Windows 2000 дает разрешения Print (Печать) каждому члену системной группы Everyone (Все), позволяя всем пользователям посылать документы на принтер. Вы также можете назначать разрешения доступа к принтерам отдельным пользователям или группам. Вы вправе изменять заданные по умолчанию или назначенные Вами ранее разрешения для любого пользователя или группы.

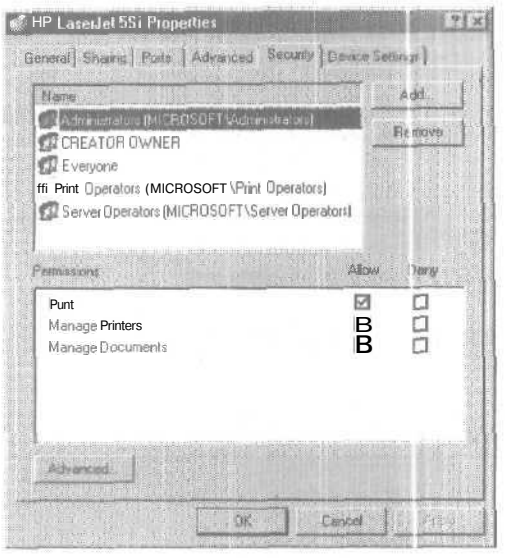


Рис. 8-8. На вкладке Security (Безопасность) диалогового окна свойств HP LaserJet 5Si указаны стандартные разрешения для принтера

Управление **принтерами**

Подразумевает выбор форм для лотков с бумагой и включение страницы-разделителя. Кроме того, при возникновении неисправности на устройстве печати Вы можете приостанавливать, возобновлять и отменять как печать конкретного документа, так и всех заданий в очереди печати. Если устройство печати неисправно или Вы устанавливаете в сети дополнительные устройства печати, Вам может понадобиться перенаправить документы на другой принтер. Вы также можете назначить определенного человека ответственным за администрирование принтеров, сделав его их владельцем.

Назначение форм лоткам с бумагой

Если в устройстве печати несколько лотков для бумаги разных форматов, Вы можете задать для лотка форму, определяющую размеры бумаги и полей. Затем пользователи смогут выбирать размер бумаги при печати из приложений, а Windows 2000 автоматически направит задание печати на лоток с нужной формой. В качестве примеров форм можно привести Legal, Letter, A4 и Executive.

Чтобы назначить форму для лотка, выберите принтер в папке Printers (Принтеры), а затем в меню File (Файл) — команду Properties (Свойства). В диалоговом окне свойств выбранного принтера перейдите на вкладку Device Settings (Параметры устройства), где и задаются формы (рис. 8-9).

На рис, 8-9 некоторые функции недоступны, поскольку они не установлены либо неприменимы для данного принтера. Функции на вкладке Device Settings, зависят от драйвера принтера, Например, персональный лазерный принтер HP LaserJet 5L допускает только два типа подачи бумаги: автоматическую и ручную.

СЕТЕВАЯ АКАДЕМИЯ ЛАНИТ

Microsoft GOLD CERTIFIED Partner | Learning Solutions

Учебный Центр «Сетевая Академия ЛАНИТ»
1осква, ул. Доброслободская, 5 тел. (095) 967-6670, факс. (095) **265-5101,** e-mail:academy@academy.ru, http://www.academy.ru

Предъявитель этого *купона получит*

20% СКИДКУ *при записи на любой из наиболее популярных 5-дневных курсов Microsoft в* **«Сетевой Академии ЛАНИТ»**

Список курсов, на которые распространяется данное предложение:

Тема	Курсы Microsoft
Microsoft Windows Server 2003	**2274** Управление средой Microsoft* Windows® Server 2003 **2275/76** Поддержка среды Microsoft® Windows™ Server 2003/Внедрение сетевой инфраструктуры Microsoft* Windows® Server 2003: Сетевые узлы **2277** Внедрение, Управление и Поддержка сетевой инфраструктуры Microsoft® Windows® Server 2003: Сетевые службы **2278** Планирование и Поддержка сетевой инфраструктуры Microsoft® Windows® Server 2003 **2279** Планирование, Внедрение и Поддержка Службы каталогов Active Directory Microsoft® Windows™ Server 2003
Microsoft Windows 2000	**2152** Внедрение Microsoft® Windows® 2000 Professional и Server **2153** Внедрение сетевой инфраструктуры Microsoft® Windows™ 2000 **2154** Внедрение и администрирование службы каталогов Microsoft® Windows* 2000
Microsoft SQL Server 2000	**2072** Администрирование баз данных Microsoft® SQL Server 200C **2073** Программирование баз данных в Microsoft® SQL Server 2000
Microsoft Exchange Server	**1572** Администрирование и системная поддержка Microsoft® Exchange 2000 **2400** Внедрение и управление Microsoft Exchange Server 2003
Supporting users	**2261/62** Поддержка пользователей, работающих с операционной системой Microsoft* Windows'" XP / Поддержка пользовательских приложений, работающих под управлением операционной системы Microsoft® Windows® XP
Project Management	**2732** Планирование, развертывание и управление Решениями по Управлению Проектами предприятия

Учебный Центр «Сетевая Академия ЛАНИТ»
Москва, ул. **Доброслободская,** 5 **тел.** (095) 967-6670, **факс.** (095) **265-5101,** e-mail:academy@academy.ru, **http://www.academy.ru**

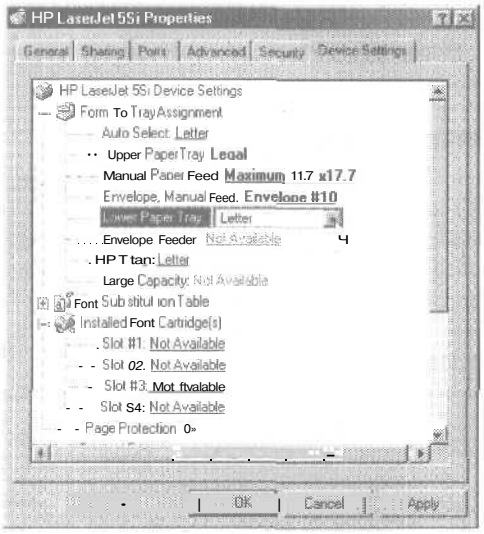


Рис. 8-9. Вкладка Device Settings (Параметры устройства) для принтера HP LaserJet 5Si

Настройка страницы-разделителя

Страница-разделитель — это файл, содержащий команды устройства печати. Страницы-разделители имеют два назначения:

- идентификация и разделение печатаемых документов;
- переключение между режимами печати; страницы-разделители позволяют выбрать язык описания страниц: например, устройству печати, которое может переключаться между режимами печати, но неспособно автоматически определить язык задания печати, можно указать применение языка PostScript или PCL.

В Windows 2000 четыре файла страниц-разделителей. Они хранятся в папке %system-root%\System32. Вот их имена и функции:

Имя файла	Функция
Pcl.sep	Переводит устройства печати серии HP в режим печати PCL, а также печатает страницу перед каждым документом.
Pscript.sep	Переводит устройства печати серии HP в режим печати PostScript, не печатая страницу перед документом.
Sysprint.sep	Печатает страницу перед каждым документом. Совместим с устройствами печати PostScript.
Sysprtj.sep	Версия файла Sysprint.sep, использующая **японские** символы.

Вы можете разработать собственную страницу-разделитель, создав sep-файл, содержащий допустимые команды принтера. Вы также можете изменить существующий sep-файл, чтобы он соответствовал Вашим потребностям. Сведения о командах, допустимых для Вашего принтера, приведены в его документации.

Если Вы решили использовать страницу-разделитель и выбрали подходящую, перейдите на вкладку Advanced (Дополнительно) в окне свойств принтера и щелкните кнопку

Separator Page (Страница разделитель). В одноименном диалоговом окне введите имя страницы-разделителя или укажите путь к ее файлу. После настройки страницы-разделителя она будет печататься в начале каждого задания на печать.

Приостановка, возобновление и отмена печати документов

Иногда требуется приостановить или возобновить печать документа или отменить печать всех документов в очереди.

Все эти задачи можно выполнить из окна Printers (Принтеры). Щелкните значок устройства печати, раскройте меню File (Файл) и выберите команду Pause Printing (Приостановить печать) или Cancel All Documents (Очистить очередь печати).

В таблице описаны задачи администрирования принтера, способы их выполнения и примеры ситуаций, когда в этом возникает необходимость.

Задача	Способ выполнения	Пример
Приостановка печати	Выберите команду Pause Printing (Приостановить печать). Против этой команды появится галочка, означающая, что печать приостановлена.	Приостановите печать в случае неисправности принтера или устройства печати. После устранения неисправности печать можно продолжить.
Возобновление печати	Снова щелкните Pause Printing (Приостановить печать). В результате галочка против этой команды исчезнет - печать возобновлена.	Устранив неисправность принтера или устройства печати, возобновите печать.
Отмена печати всех документов	Щелкните Cancel All Documents (Очистить очередь печати) — все документы будут удалены из очереди печати.	Отмените печать всех документов для очистки очереди от накопившихся старых документов, которые не нужно распечатывать.

Примечание Печать можно также приостановить, переведя принтер в автономный режим. В этом случае все документы останутся в очереди печати, даже при завершении работы и последующем перезапуске сервера печати. Чтобы перевести принтер в автономный режим, откройте окно этого принтера и в меню Printer (Принтер) выберите команду Use Printer Offline (Отложенная печать).

Направление документов на другой принтер

Документы могут быть перенаправлены на другой принтер. Например, если принтер соединен с неисправным устройством печати, можно направить печатаемые на нем документы на другой принтер, чтобы пользователям не пришлось повторно посылать их на печать. На другой принтер можно направить только всю очередь печати целиком, но не отдельные документы. При этом новый принтер должен использовать тот же драйвер, что и текущий.

Чтобы направить документы на другой принтер, откройте диалоговое окно свойств текущего принтера. Выберите вкладку Ports (Порты) и добавьте порт.

Если на текущем сервере печати есть другое устройство печати, Вы можете продолжить использовать тот же принтер, привязав его к другому устройству печати. Чтобы при-

вязать принтер к сетевому или локальному устройству печати, использующему тот же драйвер принтера, выберите соответствующий порт на сервере печати и снимите выделение с текущего порта. Документы, которые уже начали печататься, не могут быть направлены на другой принтер.

Владение принтером

По умолчанию владельцем принтера считается установивший его пользователь. Если он больше не может администрировать принтер (например, при увольнении из организации), то владение должно быть передано другому пользователю.

Владеть принтером вправе:

- пользователи, обладающие разрешением Manage Printers (Управление принтерами) для принтера, или член группы с таким разрешением;
- члены групп Administrators (Администраторы), Print Operators (Операторы печати), Server Operators (Операторы сервера) и Power Users (Опытные пользователи), так как по умолчанию эти группы имеют разрешения Manage Printers (Управление принтерами).

Для назначения владельца принтера щелкните кнопку Advanced (Дополнительно) на вкладке Security (Безопасность) диалогового окна свойств принтера. Пользователь принтера не вправе назначить владельцем принтера другого пользователя. Однако администратор может предоставить владение группе Administrators.

Для отслеживания как успешных, так и неуспешных попыток завладеть принтером применяется аудит. Как и передача владения, аудит относится к расширенным функциям системы безопасности: щелкните кнопку Advanced на вкладке Security диалогового окна свойств принтера.

Управление документами

Windows 2000, помимо управления принтерами, позволяет управлять и документами: приостанавливать, возобновлять, повторять и отменять их печать, что удобно при устранении неполадок. Вы также можете посылать уведомления о завершении выполнения задания печати и задавать уровень приоритета документа (что позволяет напечатать критически важный документ перед всеми остальными) и время его печати.

Приостановка, повтор и отмена печати документа

При возникновении проблемы с печатью отдельного документа Вы можете приостановить, а затем возобновить его печать. Вы также можете отменить печать или снова начать печатать документ, для чего Вы должны обладать разрешением Manage Documents (Управление документами) для соответствующего принтера. Поскольку создатель документа по умолчанию получает разрешения на управление им, пользователи могут выполнять над своими документами все описанные выше действия.

Чтобы произвести какое-либо действие по управлению документом, откройте окно принтера и выберите нужный документ. Щелкните меню Document (Документ), а затем — соответствующую команду для приостановки, возобновления, повтора или отмены печати документа.

В таблице описаны задачи администрирования индивидуальных документов и способы их выполнения.

Задача	Способ выполнения	Пример
Приостановка печати документа	Щелкните документ правой кнопкой мыши и выберите в контекстном меню команду Pause (Пауза) — статус документа изменится на Paused (Приостановлен).	Приостановите печать, если при печати документа возникли проблемы.
Возобновление печати документа	Щелкните документ правой кнопкой мыши и выберите в контекстном меню команду Resume (Продолжить) — статус документа изменится на Printing (Идет **печать).**	Устранив проблему, возобновите приостановленную печать.
Повтор печати документа	Щелкнув документ правой кнопкой, выберите команду Restart (Перезапустить) — документ будет напечатан заново.	Повторите печать частично напечатанного документа после устранения проблемы.
Отмена печати документа	Щелкнув документ правой кнопкой, выберите команду Cancel (Отменить); отменить печать можно, нажав клавишу Delete.	Отмените печать, если документ содержит неверные значения параметров принтера или его не надо печатать.

Настройка уведомления, приоритета и времени печати

Заданиями печати можно управлять и с помощью уведомлений, приоритетов и указывая время печати. При этом Вы должны иметь разрешение Manage Documents для соответствующего принтера.

Для настройки уведомления, приоритета или времени печати откройте диалоговое окно свойств задания печати и перейдите на вкладку General (Общие). Сначала откройте окно соответствующего принтера в папке Printers (Принтеры), щелкните документ правой кнопкой мыши и выберите в контекстном меню команду Properties (Свойства).

В таблице описаны задачи администрирования заданий печати и способы их выполнения.

Задача	Способ **выполнения**	Пример
Настройка уведомления	В поле Notify (Уведомление) введите имя пользователя, который должен получить уведомление. По умолчанию уведомляется пользователь, печатающий документ.	Измените уведомление о печати, если копию документа должен получить кто-то еще.
Изменение приоритета документа	Ползунком Priority (Приоритет) укажите уровень приоритета; самый высокий — 99, самый низкий — 1.	Измените уровень приоритета, чтобы важный документ печатался в первую очередь.
Планирование времени печати	Чтобы ограничить время, в течение которого документ может печататься, щелкните Only From (только с) в области Schedule (Расписание), а затем задайте временной интервал, когда документ может печататься.	Задайте время печати для большого документа, чтобы он печатался в период минимальной нагрузки, например ночью.

Управление принтерами из обозревателя Web

Windows 2000 позволяет управлять принтерами с любого компьютера, на котором установлен обозреватель Web. На этом компьютере не требуется даже наличия Windows 2000 или драйвера принтера. С помощью любого распространенного обозревателя, выполняющегося на любой клиентской платформе, пользователи могут просматривать Web-страницы, отражающие статус сервера печати Windows 2000 и подключенных к нему принтеров. Из обозревателя можно выполнять те же задачи управления, что и с помощью инструментов управления Windows 2000. Отличие администрирования при этом заключается в использовании Web-интерфейса. Чтобы сервер печати Windows 2000 Server поддерживал Web-страницы, на компьютере, где расположен принтер, должны быть установлены службы Microsoft Internet Information Services (IIS). Для поддержки Web-страниц сервером печати Windows 2000 Professional компьютер должен быть сконфигурирован с помощью Microsoft Peer Web Server (PWS).

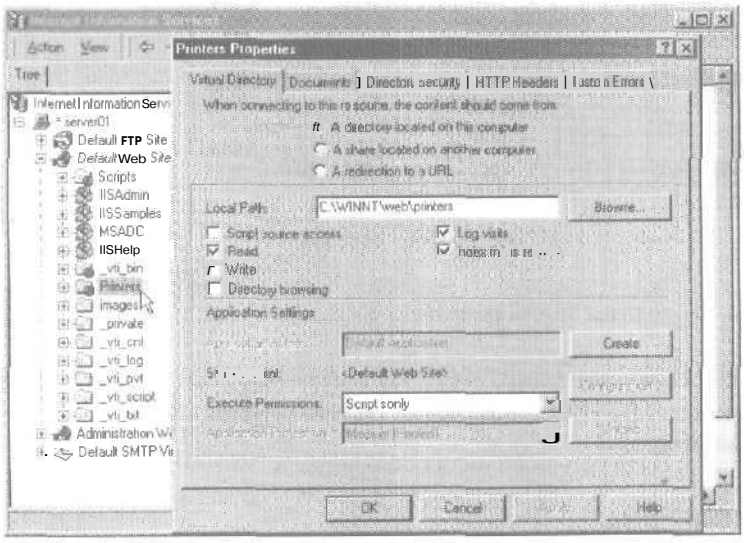


Рис. 8-Ю. Вкладка Virtual Directory (Виртуальный каталог) диалогового окна Printers Properties (Свойства: Printers)

При установке IIS создается виртуальный подкаталог Printers в рамках Web-узла по умолчанию (рис. 8-10). Этот виртуальный каталог указывает на папку %system-root%\web\printers.

Преимущества использования обозревателя Web для управления принтерами

- Управление принтерами с любого компьютера, на котором установлен обозреватель Web. На этом компьютере не требуется даже наличия Windows 2000 или драйвера принтера.
- Гибкая настройка интерфейса. Например, можно создать собственную Web-страницу, содержащую план этажа с расположением принтеров и связей с ними.
- Позволяет создать страницу, отражающую статус всех принтеров на сервере печати.
- Получение сведений об устройстве в режиме реального времени: например, пребывает ли принтер в режиме экономии электроэнергии (если драйвер способен выдать такую информацию). Из окна Printers (Принтеры) эти данные получить нельзя.

Доступ к принтерам из обозревателя Web

Для доступа ко всем принтерам на сервере печати, откройте обозреватель Web и введите адрес *http://<сервер_печати>/printers*.

Если Вы хотите получить доступ к определенному принтеру, не просматривая список всех принтеров, введите адрес *http://<сервер_печати>/<ресурс>*На рис. 8-11 изображена Web-страница, появляющаяся при доступе к принтеру Printer1 на сервере Server01. Заметьте: адрес *http://Server01/printer1*набранный в адресном поле, через активную страницу сервера (active server page, ASP) перенаправляется на *http://server01/printers/ipp_0004.asp?eprinter=Printer1&view=q&page=1139*.

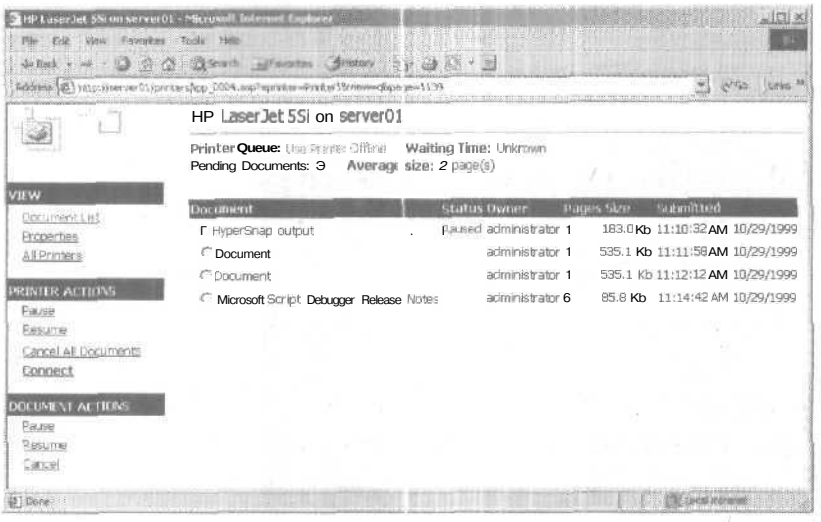


Рис. 8-11. Web-страница принтера HP LaserJet 5Si на сервере ServerOl с перечнем документов

Создание пула принтера

Пул принтера (printer pool) — это принтер, к которому подсоединено несколько локальных или сетевых устройств печати через порты на сервере печати, Эти устройства не должны быть идентичными, но должны использовать один и тот же драйвер принтера. На рис. 8-12 показан пул принтера с тремя устройствами печати.

При наличии пула пользователи могут печатать документы, не выясняя, какое из устройств печати доступно, — за них это делает принтер. Чтобы создать пул принтера, в диалоговом окне свойств принтера перейдите на вкладку Ports (Порты). На ней выберите или создайте порты, содержащие устройства печати в составе пула, и пометьте флажок Enable Printer Pooling (Разрешить группировку принтеров в пул) в низу страницы.

Примечание Создавая пул принтера, расположите входящие в него устройства печати по соседству — пользователи тогда легко найдут распечатанные документы. В противном случае они не будут точно знать, где были распечатаны их документы. Хотя, может, это и к лучшему — дополнительная физическая нагрузка им не повредит.

Пул принтера:

- позволяет сократить время, в течение которого документ находится на сервере печати в ожидании печати; это особенно важно, если в сети печатается много документов;

- упрощает администрирование, так как управлять несколькими устройствами печати можно через один принтер.

Перед созданием пула убедитесь, что все устройства печати подключены к серверу печати либо к сети.

Рис. 8-12. Печать через пул, содержащий три устройства печати

Приоритеты принтеров

Подразумевает определение приоритетов для документов, печатающихся на одном устройстве печати. Если на одно устройство печати указывают несколько принтеров, пользователи могут посылать важные документы на принтер с высоким приоритетом, а остальные — на принтеры с более низким. Первыми всегда будут печататься важные документы.

Чтобы задать приоритеты принтеров, привяжите несколько принтеров к одному устройству печати, то есть к одному порту. Это может быть как физический порт на сервере печати, так и порт, указывающий на сетевое устройство печати. Для каждого принтера, соединенного с устройством печати, определите уникальное значение приоритета, а затем прикрепите разные типы пользователей или разные типы документов к разным принтерам.

Устранение типичных проблем печати

Обнаружив проблему, сначала проверьте кабели и питание принтера, а также соединение принтера с сервером печати. Если устройство печати сетевое, убедитесь в наличии сетевого соединения между ним и сервером печати.

Чтобы обнаружить источник проблемы, попытайтесь сначала распечатать документ из другой программы — не исключено, что «виновато» ПО. Если проблема все же в принтере, ответьте на следующие вопросы:

- Возникают ли у других пользователей проблемы при печати на этом принтере и устройстве печати?
- Правильный ли драйвер использует для этого устройства сервер печати?
- Исправен ли сервер печати и хватает ли места на диске для размещения очереди печати?
- Правильный ли драйвер принтера установлен на клиентском компьютере?
- Запущены ли на сервере печати службы Print Spooler и Remote Procedure Call (RPC)?

Свойства сервера печати

Если Вы подозреваете, что проблема заключается в сервере печати, откройте окно Printers (Принтеры) и выберите в меню File (Файл) команду Server Properties (Свойства сервера). Диалоговое окно свойств сервера печати позволяет настроить формы, параметры портов, установленные драйверы принтера и дополнительные параметры, например папку очереди печати.

По умолчанию папкой очереди печати является %systemroot%\System32\spool\PRINTERS. Если на сервер печати ложится большая нагрузка, переместите папку с загрузочного раздела диска в другое место. Если загрузочный раздел заполнится до предела заданиями, печать остановится и, что хуже, ОС начнет сбоить.

Обзор типичных проблем печати

Ряд проблем встречается в большинстве сред сетевой печати. Вот некоторые из них.

Проблема	Возможная причина	Решение
Пользователь получает сообщение об отказе в доступе при попытке конфигурирования принтера из приложения, например из ранней версии Microsoft Excel.	У пользователя нет соответствующих разрешений на изменение конфигурации принтера.	Измените разрешения пользователя или сами сконфигурируйте принтер.
Документ не печатается вообще или печатается в искаженном виде.	Неправильный драйвер принтера.	Установите соответствующий драйвер принтера.
Жесткий диск на сервере переполнен, и документ не достигает устройства печати.	На диске не хватает места для очереди печати.	Освободите место печати на жестком диске сервера печати или разместите папку с заданиями печати в свободном разделе.
Тестовая страница не печатается, хотя устройство печати правильно подсоединено и включено.	Выбран неправильный порт.	Укажите правильный порт принтера. Если принтер использует сетевое устройство печати, убедитесь, что сетевой адрес задан верно.
При печати через сервер печати Windows 2000 пользователи получают сообщение об ошибке с требованием установить драйвер принтера.	На сервере печати не установлены драйверы принтера для клиентских компьютеров.	На сервере печати установите соответствующие драйверы принтера для клиентских компьютеров. Для этого используйте компакт-диск с ОС клиентского компьютера или запросите драйвер принтера у поставщика.
Документы с одного из клиентских компьютеров не печатаются, однако при печати с других клиентских компьютеров проблем не возникает.	Клиентский компьютер соединен не с тем принтером.	На клиентском компьютере удалите неправильный принтер, а затем установите корректный.

(окончание)

Проблема	Возможная причина	Решение
Документы нормально печатаются на некоторых, но не на всех устройствах печати в пуле принтера.	В пул принтера включены неидентичные устройства печати.	Убедитесь, что устройства печати, входящие в пул, идентичны либо используют одинаковые драйверы принтера. Если это не так, удалите из пула несовместимые устройства.
Документы печатаются не в порядке их приоритетов.	Неверно заданы приоритеты принтеров печати.	Установите корректные приоритеты принтеров, связанных с устройством.

Резюме

Для администрирования принтеров применяется окно Printers (Принтеры), открываемое из меню Start (Пуск), оснастка Active Directory Users And Computers (Active Directory — пользователи и компьютеры) или обозреватель Web. В Microsoft Windows 2000 управление и администрирование принтеров осуществляется посредством разрешений. Управление принтерами включает в себя задание форм для лотков с бумагой и определение страницы-разделителя. При неисправности устройства печати Вы можете приостанавливать, возобновлять и отменять задания печати. Вы можете управлять документами, включая приостановку, возобновление, повтор и отмену печати документа. Windows 2000 позволяет управлять принтерами с любого компьютера, на котором установлен Web-браузер, причем для этого даже не требуется Windows 2000 или драйвер принтера, Вы также можете создать пул принтера для объединения нескольких устройств печати. Приоритеты принтеров позволяют установить порядок печати разных групп документов. На этом занятии мы также рассмотрели способы устранения типичных проблем печати, например отказ в печати документа или отсутствие доступа к устройству печати,

Занятие 4. Печать и Active Directory

Служба каталогов призвана облегчить пользователям процесс поиска принтеров. Подсистема печати Windows 2000 тесно интегрирована в Active Directory, что позволяет искать в домене принтеры, находящиеся в разных местах.

Изучив материал этого занятия, Вы сможете:

- ✓ описать интеграцию подсистемы печати в Active Directory.

Продолжительность занятия — около 20 минут.

Обзор печати и Active Directory

Active Directory представляет собой распределенную базу данных, совместно используемую контроллерами доменов в сети. Хранилище Active Directory содержит сведения об именах принтеров, их расположении и очередях заданий печати. Эта информация рассылается на индивидуальные серверы печати, поэтому в Active Directory должны содержаться самые свежие данные о принтерах.

Важнейшие характеристики взаимосвязи серверов печати и службы Active Directory:

- каждый сервер печати отвечает за публикацию своих принтеров в хранилище Active Directory;
- сервер печати не прикреплен к определенному контроллеру домена — он динамически находит контроллер в нужном домене;
- при обновлении принтера на сервере печати эти изменения автоматически отражаются в хранилище Active Directory;
- принтеры публикуются в Active Directory как объекты printQueue; в опубликованном объекте printQueue содержится часть сведений о принтере, хранимых на сервере печати.

Для совместной работы печати и Active Directory административного вмешательства не требуется. Вносить изменения в стандартный механизм их взаимодействия следует только в случае необходимости. Особенности функционирования этого механизма таковы:

- любой принтер, управляемый сервером печати, публикуется в Active Directory; для установки и предоставления совместного доступа к этому принтеру по-прежнему требуется административный доступ к несущему (host) компьютеру;
- в хранилище Active Directory объект printQueue помещается в объект сервера печати;

Примечание В оснастке Active Directory Users And Computers (Active Directory — пользователи и компьютеры) Вы не увидите объект принтера под объектом Computer. Чтобы увидеть принтер, связанный с сервером печати, выберите в этой оснастке команду Find (Найти).

- при изменении конфигурации принтера его объект в Active Directory обновляется автоматически, а в хранилище Active Directory посылаются все данные о конфигурации принтера, включая и те, что не были изменены;
- при удалении сервера печати из сети все связанные с ним принтеры удаляются из Active Directory.

Публикация принтеров Windows 2000

Публиковать разрешено только совместно используемые принтеры. Для публикации принтера пометьте флажок List In The Directory (Перечислить в Папка) на вкладке Sharing (Доступ) (рис. 8-7).

Мастер Add Printer (Установка принтера) не позволяет изменять этот параметр при установке принтера. Принтеры, добавленные с помощью этого мастера, публикуются по умолчанию. Если Вы не хотите публиковать принтер в Active Directory, сбросьте флажок List In The Directory.

Примечание Устройство печати, подключенное через порт шины USB, скорее всего будет обнаружено автоматически, что повлечет за собой автоматическую установку принтера для этого устройства печати. При этом Вы должны на вкладке Sharing (Доступ) вручную открыть совместный доступ к принтеру и опубликовать его.

В Active Directory принтер помещается в объект сервера печати. Принтер, размещенный в Active Directory, можно переименовать или переместить из диалогового окна Find Printers (Поиск: Принтеры). Это окно можно открыть из оснастки Active Directory Users And Computers (Active Directory — пользователи и компьютеры), выбрав в меню Action (Действие) команду Find (Найти). В раскрывающемся списке Find (Найти) выберите принтеры и щелкните кнопку Find Now (Найти). На рис. 8-13 показано, как переместить принтер, используя диалоговое окно Find Printers (Поиск: Принтеры).

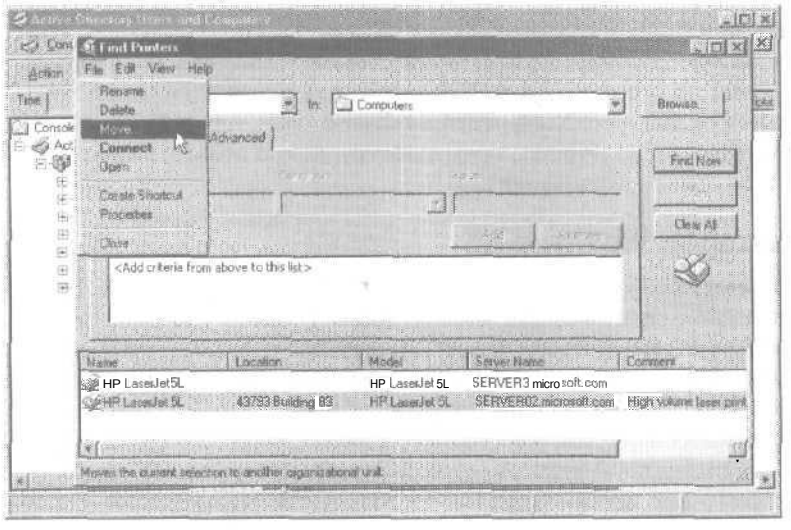


Рис. 8-13. Перемещение принтера в диалоговом окне Find Printers

Механизм опубликования

Сервер печати передает данные в Active Directory асинхронно. Сначала он посылает данные с задержкой в 1 секунду. Если эта попытка не удается, он снова посылает данные, но уже через более длительный интервал. Так будет продолжаться, пока время задержки не достигнет 2 часов. Затем данные будут посылаться через интервал этой длины, вплоть до успешной передачи. Все это время на вкладке Sharing (Доступ) диалогового окна свойств принтера Вы будете видеть сообщение «The Directory operation is still in progress».

Принтер публикуется в произвольный контроллер домена, поэтому пока он не будет реплицирован на все контроллеры домена, запрос может его не обнаружить. Для локальных контроллеров домена, находящихся в том же узле, максимальное время задержки — 30 минут, хотя обычно составляет 5-10 минут. При поиске в других узлах время задержки зависит от стратегии репликации, применяемой в Вашей организации.

Отсечение принтеров

Когда принтер удаляется с сервера печати, соответствующий объект в Active Directory также должен быть удален. За это отвечает программа отсечения принтеров, которая выполняется на каждом контроллере домена, периодически проверяя наличие удаленных принтеров. Если принтер не существует, соответствующий ему объект удаляется. Программа отсечения принтеров проверяет только серверы печати, находящиеся в том же узле, что и контроллер домена, на котором она выполняется.

Поведение программы отсечения принтеров определяется несколькими параметрами системных правил. По умолчанию действует следующее правило: если обнаружить принтер нельзя три раза подряд при проверке через каждые 8 часов, предполагается, что принтера больше нет, и он удаляется.

Однако бывает, что принтер становится недоступным лишь на некоторое время — например, при реконструкции или выключении сервера печати. В этом случае объекты принтера также должны быть удалены, так как хранилище Active Directory должно содержать сведения только об актуальных устройствах печати. Но как только сервер возобновит функционирование, его принтеры должны быть снова опубликованы. Чтобы избежать проблем в таких ситуациях, при каждом перезапуске сервера печати и запуске спулера сервер печати проверяет, все ли его принтеры опубликованы. Можно выполнить принудительный перезапуск командами net stop spooler и net start spooler или из оснастки Group Policy: раскрыв папки Computer Configuration (Конфигурация компьютера), Administration Templates (Административные шаблоны), Printers, примените групповую политику Check Published State (Проверять состояние публикации).

Поддержка принтеров Windows NT

Принтеры на серверах печати под управлением Windows NT 4.0 или Windows NT 3.51 можно опубликовать в Active Directory с помощью оснастки Active Directory Users And Computers. В ней объект принтера создается в *организационном подразделении* (organizational unit, OU), в объекте-контейнере либо в узле домена. Создание объекта принтера во многом похоже на создание объекта пользователя или группы. Опубликовать принтер можно также, используя файл сценария Pubprn.vbs, находящийся в системной папке System32. При его выполнении надо задать два параметра: имя компьютера — сервера печати или UNC-имя (\\<*имя_компьютера*>\<*имя_сетевого_ресурса*>)и путь ADSI, указывающий, где будут храниться опубликованные данные. Вы можете публиковать как все принтеры сервера, так и отдельные принтеры. Так, чтобы с помощью Pubprn.vbs опубликовать в ОП Sales домена microsoft.com общий принтер \\Server03\5L, установленный на Windows NT Server, в командной строки введите:

```
cscript %systemroot%\system32\pubprn.vbs \\server03\5L "LDAP:/
OU=Sales,DC=microsoft,DC=com"
```

Примечание Эта команда неприменима для публикации принтеров, установленных на сервере печати Windows 2000.

Параметры групповой политики

В Active Directory входит набор правил, относящихся к печати. Они находятся в папке Computer Configuration (Конфигурация компьютера) оснастки Group Policy под Administration Templates. Для просмотра описания политики откройте диалоговое окно свойств нужного Вам правила и перейдите на вкладку Explain (Объяснение).

Отслеживание размещения принтера

Пользователи могут по атрибутам принтеров искать и находить принтеры, расположенные в нужном им месте. Это позволяет разработать схему расположения и привязать компьютеры и принтеры к определенным местам в Вашей схеме. Отслеживание размещения переопределяет стандартный метод обнаружения и связывания пользователей и принтеров, основанный на применении IP-адреса и маски подсети компьютера для оценки его физического местоположения и близости к другим компьютерам. Для активизации отслеживания размещения принтера для группы компьютеров применяется групповая политика Pre-Populate Printer Search Location Text (Заполнение строки поиска принтеров). Подробнее об отслеживании размещения принтера и настройке этой функции см. справочную систему Windows.

Резюме

Подсистема печати Windows 2000 интегрирована в Active Directory, что позволяет искать в домене принтеры, расположенные в разных местах. Для совместной работы печати и Active Directory административного вмешательства не требуется. Любой принтер, управляемый сервером печати, публикуется в Active Directory — объект printQueue помещается в объект сервера печати. При изменении конфигурации принтера обновляется объект Active Directory. Когда принтер удаляется с сервера печати, удаляется и соответствующий объект в Active Directory. Публиковать разрешено только общие принтеры. Для публикации принтера пометьте флажок List In The Directory (Перечислить в Папка) на вкладке Sharing (Доступ) в диалоговом окне свойств принтера. Принтеры на серверах печати Windows NT 4.0 или Windows NT 3.51 можно опубликовать в Active Directory с помощью оснастки Active Directory Users And Computers или сценария Pubprn.vbs. В Active Directory также входит набор групповых политик, относящихся к печати.

Замятие 5. Соединение с сетевыми принтерами

После настройки сервера печати, а также необходимых драйверов принтеров пользователи на клиентских компьютерах с Windows 9x, Windows NT и Windows 2000 могут легко подключаться к принтерам и печатать на них. На большинство клиентских компьютеров под управлением Windows драйвер принтера загружается автоматически при соединении с принтером, если, конечно, на сервере печати есть нужные драйверы.

Другие клиентские компьютеры, способные обращаться к сетевому ресурсу или печатать по IP-адресу, могут использовать принтеры, сконфигурированные для совместного использования на сервере печати Windows 2000 Server, Функциями прозрачного подключения к принтеру обладают только компьютеры под управлением Windows 9x, Windows NT и Windows 2000.

Изучив материал этого занятия, Вы сможете:

- ✓ подключиться к сетевому принтеру, используя мастер Add Printer или обозреватель Web;
- ✓ **описать процесс** загрузки драйверов **принтера.**

Продолжительность занятия — около 15 минут.

Использование мастера Add Printer

По умолчанию после установки принтера и разрешения к нему совместного доступа подключаться к этому принтеру и печатать на нем документы могут все пользователи. Способ подключения к принтеру зависит от клиентского компьютера. Клиентские компьютеры с Windows 9x, Windows NT и Windows 2000 подключаются к принтеру посредством известного Вам мастера Add Printer (Установка принтера). В Windows 2000 он наделен дополнительными функциями, хотя возможности поиска принтера и подключения к нему зависят от ОС клиентского компьютера.

Для подключения к принтеру клиентские компьютеры Windows 2000 могут также использовать обозреватель Web.

Клиентские компьютеры с Windows 2000

Используя мастер Add Printer на клиентских компьютерах с Windows 2000, Вы можете подключиться к принтеру одним из способов:

- путем поиска в Active Directory — поиск можно яести как во всем хранилище Active Directory, так и в отдельной его части; Вы можете ограничить поиск, задав некоторые свойства принтера, например возможность цветной печати; принтеры легко найти, раскрыв меню Start\Search (Пуск\Поиск) и щелкнув ярлык Printers (Принтеры);
- по UNC-имени — самый быстрый способ;
- путем поиска в сети — щелкнув кнопку Browse (Обзор).

Клиентские компьютеры с Windows 9x или Windows NT

На клиентских компьютерах под управлением Windows 9x или Windows NT в мастере Add Printer Вы можете ввести UNC-имя принтера или найти его, открыв окно Network Neighborhood (Сетевое окружение).

Примечание Существует и другой способ подключения к принтеру: выбрав в меню Start (Пуск) команду Run (Выполнить), введите UNC-имя принтера в поле Open (Открыть) и щелкните кнопку OK.

Клиентские компьютеры с другими ОС Microsoft

Пользователи клиентских компьютеров с Windows 3.x и Windows for Workgroups для подключения к принтеру вместо мастера Add Printer должны обратиться к Print Manager (Диспетчер печати).

С клиентского компьютера под управлением любой ОС Windows подключиться к принтеру можно также посредством команды:

net use lpt<x>: \\<*сервер_печати*>\<*имя_сетевого_ресурса*>

где *x* — номер порта принтера.

Для клиентов под управлением MS-DOS или OS/2 с установленным клиентским ПО Microsoft LAN Manager команда net use — единственный способ подключения к сетевому принтеру.

Эти ОС не поддерживают автоматическую загрузку драйверов при соединении с принтером. Для установки драйверов на эти клиентские компьютеры используется процедура установки драйверов ОС.

Использование обозревателя Web

Если на Вашем компьютере установлена Windows 2000, Вы можете подключиться к принтеру через корпоративную интрасеть. При этом можно обойтись без мастера Add Printer — достаточно просто ввести адрес принтера в обозревателе Web (*http://<сервер_печати>/<имя_сетевого_ресурса>*) и щелкнуть ссылку Connect на открывшейся странице. На рис. 8-14 — Web-страница по завершении соединения с принтером.

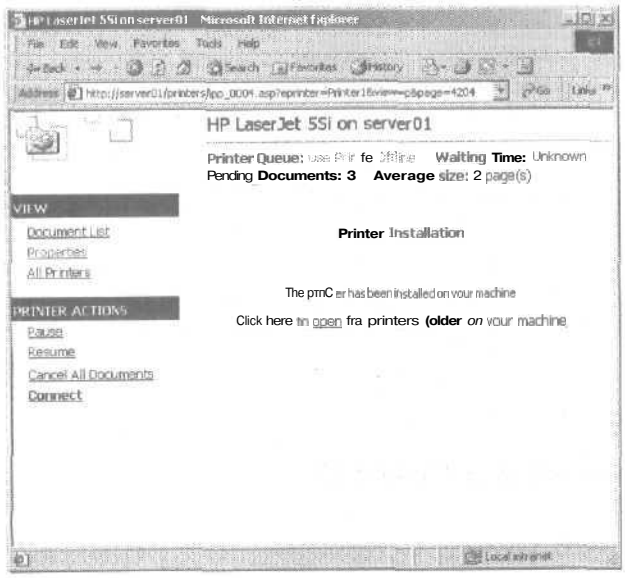


Рис. 8-14. Установка принтера и соединение с ним с помощью обозревателя Web

По завершении соединения Windows 2000 автоматически скопирует соответствующие драйверы принтера на клиентский компьютер.

Для соединения с принтером из обозревателя Web можно использовать два варианта адресов (URL):

- *http://<сервер_печати>/printers* — эта Web-страница содержит имена всех совместно используемых принтеров сервера печати, на которые Вы имеете разрешения, а также подробные сведения о принтерах: имя, статус заданий печати, местоположение, модель и комментарии, введенные при установке принтера, — это поможет выбрать наиболее подходящий принтер: впрочем, для его использования требуются соответствующие разрешения;
- *http://<сервер_печати>/<имя_сетевого_ресурса>* — адрес конкретного принтера в интрасети; чтобы использовать этот принтер, также требуются разрешения.

Разрешается самостоятельно настраивать Web-страницу для соединения с принтером. Например, Вы можете отобразить план этажа с расположением доступных устройств печати.

Чтобы сервер печати Windows 2000 принимал запросы на печать, содержащие URL, он должен быть сконфигурирован одним из следующих способов:

- с помощью Windows 2000 Server и Microsoft IIS;
- с помощью Windows 2000 Professional и Microsoft PWS.

Загрузка драйверов принтера

Когда пользователи клиентских компьютеров с Windows 9x или Windows NT впервые подключаются к принтеру на сервере печати, драйвер принтера автоматически загружается на клиент. На сервере печати должна быть установлена копия этого драйвера. Дополнительные драйверы принтера можно установить, щелкнув кнопку Additional Drivers (Дополнительные драйверы) на вкладке Sharing (Доступ) диалогового окна свойств принтера.

Для каждой платформы существуют свои драйверы принтера. Так что если Вы хотите установить поддержку подключения к принтеру и загрузки его драйвера для нескольких платформ Windows NT, не забудьте установить соответствующие драйверы. Например, для поддержки Windows NT-клиентов с процессорами Alpha и *x86* надо установить на сервер печати оба драйвера. Драйверы Windows 2000 несовместимы с драйверами Windows NT. Например, если у Вас сервер печати Windows 2000 с процессором *x86* и Вы планируете поддерживать клиентов Windows NT с процессором *x86*, установите драйверы принтера именно для Windows NT с процессором *x86*. В окне Additional Drivers (Дополнительные драйверы) для таких драйверов принтеров в столбце Environment (Переменные среды) значится Intel. Впрочем, эти драйверы работают и на альтернативных платформах.

Клиентские компьютеры с Windows 2000 и Windows NT проверяют наличие текущего драйвера принтера при каждой печати. Если текущего драйвера у них нет, они загружают его. При этом Вы должны следить лишь за обновлением драйверов принтера на сервере печати. Клиентские компьютеры с Windows 9x не проверяют наличие обновленных драйверов принтера. На эти клиенты обновленные драйверы надо устанавливать вручную.

Резюме

Клиентские компьютеры с Windows 9x, Windows NT и Windows 2000 подключаются к принтеру с помощью мастера Add Printer (Установка принтера). На клиентских компьютерах под управлением Windows 9x и Windows NT найти принтер можно по его UNC-имени либо из окна Network Neighborhood (Сетевое окружение). Клиентские компьютеры с Windows 3.x и Windows for Workgroups для подключения к принтеру задействуют Print Manager. На любом клиенте под управлением Windows или MS-DOS для подключения к принтеру применяется команда net use. Клиенты с Windows 2000 способны подключаться к принтеру путем поиска в Active Directory или сети, по UNC-имени принтера, а также с помощью Web-браузера. Клиенты Windows 9x или Windows NT при первом подключении к принтеру на сервере печати автоматически загружают драйвер принтера.

Закрепление материала

Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. В чем разница между устройством печати и принтером?

2. Ваш коллега запретил Вам удалять системную группу Everyone (Все) из разрешений принтера, иначе, по его словам, никто не сможет управлять принтером и его очередью. В чем он не прав? Как можно избежать подобной проблемы?

3. В Вашей сети два сервера печати. При подключении пользователя с Windows 95 к одному из них печать выполняется автоматически. Когда тот же пользователь подключается к этому же серверу печати, но к другому принтеру, то получает сообщение о необходимости установить драйвер. В чем причина?

4. Многие сотрудники Вашей организации используют одно устройство печати. Как избежать путаницы пользователей в документах?

5. Можно ли перенаправить на другой принтер отдельный документ?

6. Пользователю нужно напечатать очень большой документ. Как это сделать в нерабочее время, не присутствуя при печати?

ГЛАВА 9

Сетевые службы и протоколы

В этой главе

В этой главе **рассказывается** о сетевых **протоколах, поддерживаемых Microsoft Windows** 2000, включая пакет **протоколов** TCP/IP, **NWLink, AppleTalk и др. Мы также обсудим** реализацию протокола **TCP/IP и сетевых** служб **DHCP,** WINS **и DNS.**

Прежде всего

Для изучения материалов этой главы **Вам потребуется:**

- **установить Windows** 2000 **Server;**
- выполнить упражнения предыдущих глав.

Занятие 1. Сетевые протоколы

Протокол — это набор правил и соглашений о порядке передачи данных в сети. Пакеты данных перемещаются вверх и вниз по стеку протокола и в среде передачи. Мы расскажем об основных сетевых протоколах, поддерживаемых Windows 2000.

Изучив материал этого занятия, Вы сможете:

- ✓ перечислить основные сетевые протоколы, поддерживаемые Windows 2000.

Продолжительность занятия — около 15 минут.

Общие сведения о сетевых протоколах

Протокол — это набор правил и соглашений о порядке передаче информации в сети. Windows 2000 поддерживает в числе прочих протокол TCP/IP, используемый при организации доступа в сеть, для поддержки файловых служб и служб печати, репликации данных между контроллерами доменов и др. Windows 2000 также поддерживает сетевые протоколы:

- Asynchronous Transfer Mode (ATM);
- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX);
- NetBIOS Enhanced User Interface (NetBEUI);
- AppleTalk;
- Data Link Control (DLC);
- Infrared Data Association (IrDA).

Примечание Протоколов пакета Systems Network Architecture (SNA) в Windows 2000 нет — их поддерживает Microsoft SNA Server, отдельный продукт, обеспечивающий взаимодействие с мэйнфреймами IBM.

Порядок привязки протоколов

Протоколы можно добавлять, удалять и выборочно привязывать ко всем сетевым интерфейсам сервера. Порядок привязки протоколов определяется последовательностью, в которой они были установлены. Вы, однако, в любое время можете изменить порядок привязки протоколов для отдельных интерфейсов, что заметно расширяет возможности управления. Например, к одному интерфейсу могут быть привязаны протоколы TCP/IP и IPX/SPX с приоритетом протокола TCP/IP, а к другому — те же протоколы, но с приоритетом IPX/SPX. Кроме того, для отдельных сетевых интерфейсов, протоколов и их комбинаций можно произвольно включать или отключать сетевые службы. Такая избирательность позволяет системным администраторам легко создавать сверхзащищенные конфигурации сети (например, отключить все сетевые службы для общедоступных интерфейсов с прямым подключением к Интернету).

TCP/IP

В качестве стратегического транспортного протокола уровня предприятия для Windows 2000 выбран пакет протоколов TCP/IP. Задача этого пакета — упростить интеграцию сетей Microsoft уровня предприятия в широкомасштабные корпоративные, правительственные и общедоступные сети, а также обеспечить безопасность при работе в таких сетях. Подробнее о стеке протоколов TCP/IP см. занятие 2,

ATM

Протокол ATM — это усовершенствованная реализация коммутации пакетов, идеально подходящая для передачи голоса, видеоизображения и данных. Это высокоскоростная сетевая технология, передающая информацию в ячейках фиксированной длины. ATM состоит из группы связанных технологий, включающих ПО и аппаратное обеспечение, а также среду передачи, требующую логического соединения. Ячейка является пакетом фиксированной длины, содержащим 53 байта данных (рис. 9-1).

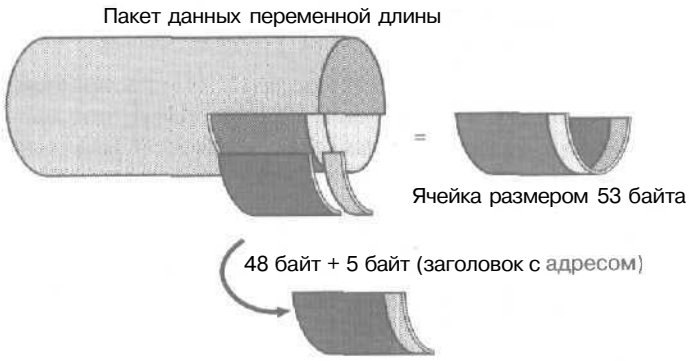


Рис. 9-1. Пакет данных размером 1 000 байт, разбитый на ячейки по S3 байта

Поскольку количество байт и, как следствие, время передачи ячейки — константы, коммутация ячеек может осуществляться через заданные промежутки времени.

Перед тем как переслать данные, ATM-терминал устанавливает связь или организует виртуальный канал. Затем терминал пересылает ячейки по созданному пути конечному узлу. Виртуальный канал представляет собой прямой путь, связывающий два терминала. При установлении соединения ATM-терминал также передает набор параметров — *качество обслуживания* (Quality of Service, QoS), который определяет полосу пропускания, максимальную задержку, допустимое отклонение и другие параметры виртуального канала и распространяется на оба терминала. Так как виртуальный канал требует логического соединения, данные прибывают на принимающий узел в определенном порядке и с заданными уровнями обслуживания. ATM — отличное компромиссное решение, обеспечивающее передачу по сети голоса и других данных. ATM гарантирует качество обслуживания в ЛВС, ГВС и других общедоступных сетях.

ATM поддерживается благодаря таким компонентам архитектуры Windows 2000, как LAN Emulation, IP поверх ATM, ATM поверх xDSL. Кроме того, используется естественный доступ к сетям ATM через Microsoft Windows Sockets (Winsock) 2.0.

LAN Emulation

Благодаря методу *LAN Emulation* (LANE, эмуляция ЛВС) через сеть ATM способны взаимодействовать протоколы, не требующие логического соединения. LANE позволяет ATM работать с устаревшими приложениями и сетями. Приложения и протоколы, способные работать с ЛВС, могут взаимодействовать через сеть ATM без дополнительных изменений.

LANE включает два основных компонента: клиент LANE (Atmlane.sys) и службы LANE. Первый размещается в папке %systemroot%\system32\drivers и позволяет протоколам ЛВС и приложениям, способным работать с ЛВС, функционировать так, будто они взаимодействуют в обычной ЛВС. Клиент LANE передает сетевым протоколам команды ЛВС, а уровню протокола ATM — «родные» команды ATM.

IP поверх ATM

Эта группа служб, обеспечивающая взаимодействие по сети ATM, — альтернатива LANE. Для переопределения структуры протокола IP, не требующей логического соединения. IP поверх ATM использует свойства ATM, которые требуют логического соединения. IP поверх ATM работает аналогично LANE. На центральном IP-сервере (сервер ATMARP) хранится база данных IP- и ATM-адресов; этот сервер предоставляет также службы конфигурирования и широковещания. Службы широковещания нужны, поскольку в протоколе ATM соответствующих функций нет. Службы IP поверх ATM находятся на разных узлах и обычно не размещаются на сервере, осуществляющем коммутацию ATM. В Windows 2000 есть все службы протокола IP поверх ATM.

Фактически IP поверх ATM — это небольшая прослойка между ATM и протоколами пакета TCP/IP. На верхнем уровне клиент эмулирует для стека TCP/IP стандартный протокол Интернета (IP), а на нижнем — передает уровням стека протоколов ATM естественные команды ATM.

Поддержка IP поверх ATM осуществляется двумя основными компонентами: *сервером ARP* (Atmarps.sys) и *клиентом ARP* (Atmarpc.sys). Сервер ARP состоит из сервера ATMARP и службы *MARS*. Сервер ATMARP предоставляет службы, эмулирующие стандартные функции протокола IP, а служба MARS — службы групповой и широковещательной рассылки. Обе поддерживают БД IP-адресов.

ATM поверх xDSL

Технология *Digital Subscriber Line* (xDSL, цифровая абонентская линия) позволяет передавать по обычной телефонной линии цифровые данные на центральную станцию телефонной компании. Для подключения пользователей DSL к магистральной сети ATM DSL-данные посылаются на *мультиплексор доступа цифровых абонентских линий* (Digital Subscriber Line Access Multiplexer. DSLAM). Дальняя часть DSLAM подключается к сети ATM, скорость передачи данных в которой измеряется в гигабитах. На другом конце каждого канала DSLAM разуплотняет сигналы и пересылает их индивидуальным DSL-соединениям.

ATM поверх xDSL обеспечивает высокоскоростной доступ к сети из дома или небольшого офиса. Для таких сред разработаны различные варианты DSL, включая *ADSL* (Asymmetric Digital Subscriber Line. асимметричная цифровая линия подписчика) и *VDSL* (Very High Digital Subscriber Line, высокоскоростная цифровая линия подписчика). В этих технологиях применяется *локальная петля — медная пара* (ADSL) или *оптоволоконный кабель* (VDSL), которая соединяет машину пользователя с ближайшей центральной станцией. Обычно локальная петля подключается прямо к основной сети ATM, обслуживаемой телефонной компанией.

Высокая скорость и надежность службы ATM поверх xDSL обеспечивается основной сетью ATM без смены протоколов. Это позволяет создать сквозную сеть ATM для дома или небольшого офиса.

Доступ к сетям ATM с помощью Winsock 2.0 и естественный доступ к сетям ATM

Поддержку протокола ATM для Winsock 2.0 обеспечивает Windows Sockets ATM Service Provider. Благодаря этому приложения, использующие в качестве транспортного протокола TCP, могут получать доступ к сетям ATM через Winsock 2.O.

Приложения, применяющие естественный протокол ATM, могут создавать виртуальные каналы, что обеспечивается добавленной в NDIS 5.0 службой *CoNDIS*, требующей логического соединения.

NWLink

Это реализация протокола IPX/SPX, разработанная Microsoft. NWLink широко применяется в средах, где Windows-клиенты обращаются к ресурсам серверов NetWare или где NetWare-клиенты обращаются к ресурсам компьютеров Windows. NWLink не позволяет компьютеру с Windows 2000 напрямую обращаться к общим файлам и принтерам сервера NetWare или выступать для клиента NetWare в качестве сервера файлов или печати. Для доступа к файлам и принтерам сервера NetWare в Windows 2000 Professional надо задействовать службу *CSNW* (Client Service for NetWare), а в Windows 2000 Server — *GSNW* (Gateway Service for NetWare).

GSNW выступает для компьютера с Windows 2000 Server, на котором она установлена, как перенаправитель, а для клиентских компьютеров — как шлюз. Шлюз позволяет компьютеру с Windows 2000 Server обращаться к ресурсам (папкам и принтерам) NetWare так, как если бы они находились на сервере с Windows 2000. Это позволяет клиентам, имеющим доступ к общим ресурсам компьютера Windows 2000 Server, обращаться к общим ресурсам, предоставляемым службой GSNW.

NWLink полезен при наличии клиент-серверных приложений NetWare, применяющих Winsock или протоколы NetBIOS поверх IPX/SPX. Кроме того, NetWare NetBIOS Link (NWNBLink) содержит усовершенствования протокола NetBIOS от Microsoft. NWNBLink форматирует запросы уровня NetBIOS и пересылает их компоненту NWLink для передачи по сети.

Выбор типа кадра

Тип кадра определяет способ предварительного форматирования данных платой сетевого адаптера, установленной на компьютере с Windows 2000, для пересылки их по сети. Для установления связи компьютеры Windows 2000 и серверы NetWare должны использовать одинаковый тип кадра.

Вот список топологий и типов кадров, поддерживаемых протоколом NWLink:

Топология	Поддерживаемые типы кадров
Ethernet	Ethernet II, 802.3, Ethernet 802.2 и Sub Network Access Protocol (SNAP), в котором по умолчанию используются кадры стандарта 802.2
Token Ring	802.5 и SNAP
FDDI	802.2 и 802.3

В сетях Ethernet стандартный тип кадра для NetWare 2.2 и NetWare 3.11 — 802.3. Начиная с NetWare 3.12, по умолчанию используется тип кадра 802.2.

Тип кадра можно выбрать вручную или настроить систему для его автоматического определения. При загрузке NWLink тип кадра определяется автоматически. Если кроме типа 802.2 обнаруживаются другие типы кадров, NWLink по умолчанию использует тип кадра 802.2. Если тип кадра задан вручную, Windows 2000 может одновременно использовать разные типы кадров.

Тип кадра можно выбрать в диалоговом окне свойств протокола NWLink. Подробнее об этом см. справочную систему Windows 2000.

NetBEUI

Протокол NetBEUI был разработан как протокол для ЛВС небольших отделов с 20–200 компьютерами. NetBEUI не поддерживает маршрутизацию, так как в его архитектуре нет сетевого уровня. Из-за этого ограничения компьютеры с Windows 2000 и NetBEUI прихо-

лится соединять мостами, а не маршрутизаторами. Кроме того, NetBEUI основан на широковещании, т. е. большинство своих функций (вроде регистрации и разрешения имен) он выполняет посредством широковещания, и поэтому объем широковещательного трафика у NetBEUI гораздо больше, чем у других протоколов. NetBEUI поставляется с Windows 2000 Server и Windows 2000 Professional для поддержки рабочих станций, не обновленных до Windows 2000.

NetBEUI обеспечивает:

- совместимость с существующими ЛВС, использующими данный протокол;
- связь между компьютерами с обязательным установлением логического соединения и без такового;
- самоконфигурирование и самонастройку;
- защиту от ошибок;
- незначительную загрузку памяти.

Примечание В сети Windows 2000 с Active Directory нельзя использовать NWLink или NetBEUI в качестве основного протокола. Для доступа к службе Active Directory может применяться лишь пакет протоколов TCP/IP.

AppleTalk

Стек протоколов AppleTalk разработан компанией Apple Computer Corporation для организации связи между компьютерами Macintosh. В Windows 2000 включена поддержка AppleTalk, позволяющая компьютерам с Windows 2000 Server и клиентам Apple Macintosh совместно использовать файлы и принтеры. Кроме того, AppleTalk позволяет Windows 2000 выступать в качестве маршрутизатора и сервера удаленного доступа.

Для корректной работы протокола AppleTalk на компьютере с Windows 2000 Server нужно установить службы Windows 2000 Services for Macintosh; компьютер также должен быть доступен в сети.

DLC

Протокол DLC разработан для организации связи между мэйнфреймами производства IBM. Он не предназначен для использования в качестве основного протокола в сети ПК. Тем не менее DLC применяется для отправки заданий печати на сетевые принтеры Hewlett-Packard. Они применяют протокол DCL, потому что получаемые кадры легко дизассемблировать и функциональность DLC легко занести в ПЗУ. DLC рекомендуется устанавливать только на сетевые компьютеры, выполняющие отправку заданий печати на сетевые принтеры Hewlett-Packard. Клиентам, посылающим задания на сетевое печатающее устройство через сервер печати Windows 2000, устанавливать протокол DLC не надо.

DLC требуется установить только на сервере печати, к которому подключено устройство печати. После установки протокола DLC на компьютере с Windows 2000 станет доступен новый тип порта принтера. Ни рис. 9-2 показан новый тип порта, появившийся в диалоговом окне Printer Ports (Порты принтера). Это окно открывается на вкладке Ports (Порты) диалогового окна свойств принтера.

На рис. 9-2 в большем окне под надписью Card Address отображается MAC-адрес (Media Access Control) серверов печати или принтеров, использующих протокол DLC. Убедитесь, что сетевое печатающее устройство с поддержкой DLC подключено к сети, включено и настроено для работы с протоколом DLC.

Когда компьютер с Windows 2000 Server будет настроен для работы в качестве сервера печати для сетевого печатающего устройства с поддержкой DLC, клиенты смогут подключаться к серверному принтеру. Если задания на устройстве печати с поддержкой DLC были посланы не через сервер печати Windows 2000 Server, возможно, что на клиенте установлен протокол DLC и задания пересылаются прямо принтеру. Для выявления компьютеров с установленным протоколом DLC служит Network Monitor (Сетевой монитор) или другой анализатор сети.

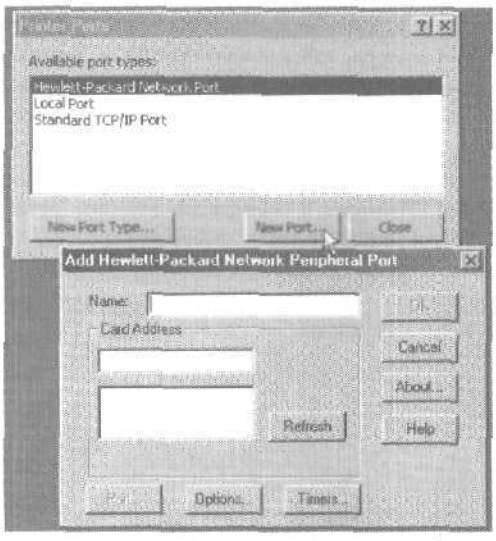


Рис. 9-2. **Диалоговое окно настройки нового сетевого принтера Hewlett-Packard, использующего протокол DLC**

Примечание В данный момент все платы JetDirect от Hewlett-Packard поддерживают TCP/IP, что позволяет добавлять такие платы через стандартный порт **TCP/IP.** Сетевой порт Hewlett-Packard, *применяющий* протокол DLC, нужен лишь устаревшим платам JetDirect, не поддерживающим **TCP/IP.**

IrDA

Представляет собой группу высокоскоростных двунаправленных инфракрасных протоколов малой дальности. Протокол IrDA обеспечивает взаимодействие различных устройств, например камер, принтеров, переносных и настольных компьютеров и *персональных цифровых помощников* (Personal Digital Assistauts, PDA). Для доступа к стеку протоколов IrDA применяются драйверы NDIS, не требующие логического соединения.

Резюме

Протокол представляет собой набор правил и соглашений о порядке передачи информации в сети. Windows 2000 поддерживает множество различных протоколов. В качестве стратегического транспортного протокола уровня предприятия для Windows 2000 выбран пакет протоколов TCP/IP. TCP/IP может передаваться по разным сетям, основанным на технологии доступа к среде, например Ethernet, Token Ring и ATM. Доступ к среде — лишь часть возможностей, предоставляемых ATM. ATM — это группа технологий (программных и аппаратных), которая обеспечивает связь с обязательным установлением логического соединения, идеально подходящую для передачи голоса, видеоизображения и данных. NWLink — используемая в Windows 2000 реализация протокола 1PX/SPX — разработана Microsoft. В Windows 2000 Professional и Windows 2000 Server также имеется протокол NetBEUI, применяемый преимущественно для поддержки рабочих станций, не обновленных до Windows 2000. Кроме того, Windows 2000 поддерживает протокол AppleTalk, позволяющий Windows 2000 выступать в качестве маршрутизатора и сервера удаленного доступа. Протокол DLC был разработан для организации связи между мэйнфреймами производства IBM; тем не менее некоторые устаревшие модели сетевых принтеров Hewlett-Packard используют этот протокол. IrDA представляет собой группу высокоскоростных двунаправленных инфракрасных протоколов малой дальности.

Занятие 2. Протокол TCP/IP

Пакет протоколов TCP/IP обеспечивает связь в сети, включающей компьютеры с различными аппаратными архитектурами и ОС. Реализация протокола TCP/IP, разработанная Microsoft, позволяет создавать сети масштаба предприятия на основе компьютеров с Windows 2000.

Изучив материал этого занятия, Вы сможете:

- ✓ рассказать о стеке протоколов TCP/IP и утилитах TCP/IP, поставляемых с Windows 2000;
- ✓ настроить TCP/IP.

Продолжительность занятия — около 60 минут.

Обзор стека протоколов TCP/IP

TCP/IP — промышленно стандартизированный пакет протоколов — позволяет создавать сети масштаба предприятия на основе компьютеров с Windows 2000. При добавлении TCP/IP в систему под управлением Windows 2000 Вы получите:

- маршрутизируемый сетевой протокол, поддерживаемый большинством ОС — TCP/IP применяется во многих крупных сетях;
- технологию, позволяющую соединять разнородные системы — для доступа и передачи данных между разнородными системами можно использовать множество стандартных утилит, доступных в том числе и в Windows 2000;
- надежную, масштабируемую, платформо-независимую структуру — TCP/IP поддерживает интерфейс Winsock, идеально подходящий для разработки клиент-серверных приложений для Winsock-совместимых стеков;
- доступ к ресурсам Интернета.

TCP/IP предоставляет набор стандартов, определяющих правила взаимодействия компьютеров и правила связи сетей. Стек протоколов TCP/IP включает 4 уровня: сетевой, Интернета, транспортный и прикладной (рис. 9-3).

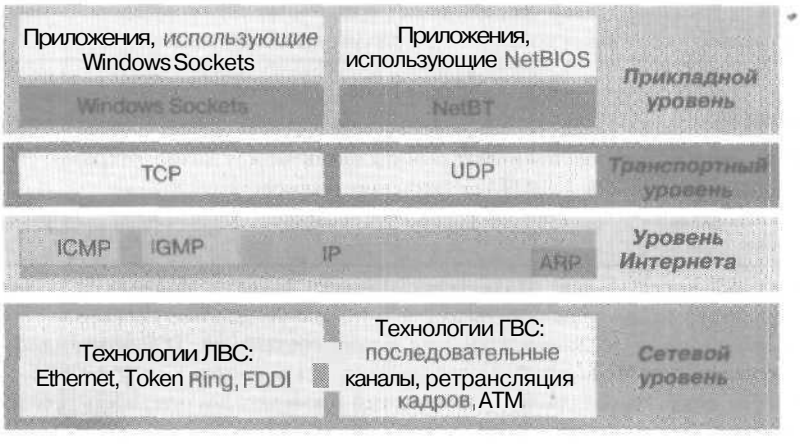


Рис. 9-3. Четыре уровня стека протоколов TCP/IP

Сетевой уровень

В основе модели лежит уровень сетевого интерфейса, принимающий и передающий кадры по физическим каналам связи.

Уровень Интернета

Протоколы уровня Интернета инкапсулируют пакеты в дейтаграммы Интернета и управляют необходимыми алгоритмами маршрутизации. 4 протокола уровня Интернета — это *IP* (Internet Protocol), *ARP* (Address Resolution Protocol), *ICMP* (Internet Control Message Protocol) и *IGMP* (Internet Group Management Protocol).

Протокол	Описание
IP	Обеспечивает доставку пакетов без установления логического соединения для остальных протоколов. Не гарантирует доставку или правильную последовательность пакетов.
ARP	Обеспечивает привязку IP-адреса к адресу подуровня MAC, что позволяет запросить физический контрольный MAC-адрес конечного узла. IP производит широковещательную рассылку специального пакета-запроса протокола ARP; этот пакет содержит IP-адрес конечной системы. Система под соответствующим IP-адресом отвечает на запрос, пересылая свой физический адрес запрашивающему устройству. Подуровень MAC взаимодействует напрямую с сетевой платой и отвечает за безошибочную пересылку данных между двумя компьютерами сети.
ICMP	Обеспечивает специальный вид связи компьютеров, позволяя им обмениваться данными о состоянии и ошибках. Протоколы более высоких уровней используют эту информацию для разрешения проблем передачи. Сетевым администраторам эти сведения помогают выявлять проблемы в сети. Утилита ping с помощью пакетов ICMP определяет, функционирует ли конкретное IP-устройство, подключенное к сети.
IGMP	Обеспечивает многоадресную рассылку (ограниченная форма широковещательной рассылки) для связи и управлением информацией между всеми устройствами группы. IGMP информирует соседние маршрутизаторы многоадресной рассылки, что в данной сети имеются члены труппы хостов. В Windows 2000 имеются возможности групповой рассылки, например, с помощью служб NetShow Services, позволяющих разработчикам создавать программы многоадресной рассылки.

Транспортный уровень

Протоколы транспортного уровня обеспечивают сеансы связи между компьютерами. Это *TCP* (Transmission Control Protocol) и *UDP* (User Datagram Protocol).

Протокол	Описание
TCP	Обеспечивает приложениям, разово пересылающим большие объемы информации или требующим подтверждения получения данных, надежную связь с обязательным установлением логического соединения. TCP гарантирует доставку пакетов, точную последовательность пакетов данных и обеспечивает вычисление контрольной суммы, позволяющей проверить достоверность приема как заголовка, так и данных пакета.

(*окончание*)

Протокол	Описание
UDP	Обеспечивает **связь без установления** логического **соединения и не гарантирует** доставку **пакетов. Приложения,** использующие **протокол UDP, разово** перелают **небольшой объем** данных, За надежность доставки **данных** отвечает **приложение.**

Прикладной уровень

Верхний уровень модели — прикладной — **предоставляет приложениям доступ к сети. В** прикладном **уровне работает множество стандартных утилит и** служб **TCP/IP: FTP, Telnet,** SNMP, **DNS и др.**

Для **взаимодействия со службами стека протоколов TCP/IP последний** предоставляет **сетевым приложениям** два интерфейса: **Winsock и NetBIOS поверх TCP/IP (NetBT).**

Интерфейс	Описание
Winsock	**Выступает** как стандартный **интерфейс между** протоколами стека **TCP/IP и приложениями,** использующими сокеты.
NetBT	**Применяется как стандартный интерфейс** для служб **NetBIOS,** включая службы **именования,** дейтаграмм и сеансов. **Обеспечивает** также стандартный **интерфейс** между **протоколами TCP/IP и приложениями на основе NetBIOS.**

Примечание О протоколе TCP/IP и его реализации см. статью \chapt09\articles\tcpip2000.doc на прилагаемом компакт-диске.

Настройка TCP/IP для использования статичного IP-адреса

По умолчанию клиенты с Microsoft Windows 2000/NT/9x **автоматически получают сведения о конфигурации TCP/IP от службы DHCP. Но даже в среде с поддержкой DHCP Вам** следует **присвоить определенным** компьютерам **статичные IP-адреса. Например,** компьютер, **на котором выполняется DHCP,** не может **быть клиентом DHCP, и поэтому ему надо присвоить статичный IP-адрес. Кроме того, если служба DHCP недоступна, TCP/IP** также следует **настроить для использования статичных IP-адресов.**

Примечание В небольших **частных сетях, где DHCP-сервер** недоступен, для автоматического **назначения IP-адресов можно применить функцию *автоматической частной IP-адресации*** **(AP1PA, Automatic Private IP** Addressing), **реализованную в Windows 2000** Server.

Для каждой **установленной на компьютере сетевой** платы, **использующей TCP/IP,** можно настроить ***IP-адрес*** **(IP** address), *маску подсети* **(Subnet mask) и *шлюз по умолчанию*** (Default gateway) **(рис. 9-4).**

Ниже описаны параметры настройки статичного TCP/IP-адреса.

Параметр	Описание
IP-адрес	Логический 32-разрядный адрес, определяющий узел TCP/IP. У каждой сетевой платы, использующей TCP/IP, должен быть уникальный IP-адрес, например, 192.168.0. 108. Любой адрес состоит из двух частей: идентификатора сети, определяющего все узлы, находящиеся в одной физической сети, и идентификатора узла, определяющего конкретный узел в сети. В нашем примере идентификатор сети — 192.168.0, а узла — 108.
Маска подсети	Одна из сетей многосетевой среды, использующая IP-адреса, выводимые из одного идентификатора сети. Подсети делят большую сеть на несколько физических сетей, соединенных маршрутизаторами. Маска подсети блокирует часть IP-адреса так, что TCP/IP может различать идентификаторы сети и хоста. При установлении связи между узлами TCP/IP маска подсети помогает определить, в какой сети находится конечный узел: локальной или удаленной. Для связи по локальной сети маски подсети компьютеров должны быть одинаковы.
Шлюз по умолчанию	Промежуточное устройство в локальной сети, хранящее идентификаторы других сетей предприятия или Интернета. Для связи с узлом другой сети следует задать IP-адрес шлюза по умолчанию. При отсутствии прочих маршрутов TCP/IP посылает пакеты для передачи в удаленную сеть через шлюз по умолчанию. Шлюз переправляет пакеты другим шлюзам до тех пор, пока пакет не попадет на шлюз, соединенный с указанным адресатом,

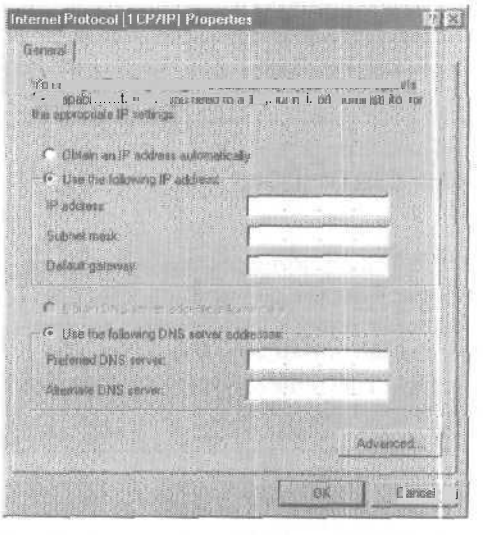


Рис. 9-4. Задание статичного TCP/IP-адреса в диалоговом окне свойств TCP/IP

Чтобы попасть в диалоговое окно свойств TCP/IP, откройте диалоговое окно свойств My Network Places (Мое сетевое окружение), затем — окно свойств требуемой сетевой платы и, наконец, окно свойств TCP/IP.

Внимание! Назначение одинаковых IP-адресов в рамках одной сети приведет к сбою IP-связи — для получения действительных статичных IP-адресов обратитесь к администратору сети.

Настройка TCP/IP для автоматического получения IP-адреса

Сервер, на котором выполняется служба DHCP, может автоматически присваивать клиентам DHCP конфигурационную информацию TCP/IP. Благодаря этому любого клиента под управлением MS-DOS, Windows 3.x, Windows for Workgroups, Windows 9x/NT/2000 можно настроить для автоматического получения конфигурационной информации TCP/IP от службы DHCP. Использование DHCP для автоматической настройки TCP/IP на клиентах упрощает администрирование и гарантирует правильность конфигурационной информации. И все же при этом надо сначала настроить компьютер как клиент DHCP.

Для этого откройте диалоговое окно свойств TCP/IP и щелкните переключатель Obtain An IP Address Automatically (Получить IP-адрес автоматически). (Подробнее о DHCP см. занятие 3.)

Использование автоматической IP-адресации

Версия стека протоколов TCP/IP, реализованная в Windows 2000, поддерживает новый механизм автоматического присвоения IP-адресов в простых конфигурациях ЛВС. Это расширение механизма динамического присвоения IP-адресов адаптерам ЛВС позволяет выделять IP-адреса без применения механизма статичных IP-адресов или установки службы DHCP.

Чтобы обеспечить корректную работу *автоматической зчастнои IP-адресации* (APIPA) на компьютере с Windows 2000, настройте адаптер ЛВС для использования TCP/IP и в диалоговом окне Internet Protocol (TCP/IP) Properties щелкните переключатель Obtain An IP Address Automatically (Получить IP-адрес автоматически). APIPA выделяет IP-адрес следующим образом,

1. TCP/IP ищет в подключенной сети DHCP-сервер, чтобы получить динамический IP-адрес.
2. Если DHCP-сервера на этапе начальной загрузки нет (например, он отключен для обслуживания или ремонта), клиент не сможет получить IP-адрес.
3. APIPA генерирует IP-адрес вида 169.254.*x.y* (*x.y* — уникальный идентификатор клиента) и маску подсети 255.255.0.0. Если выделенный адрес используется, AP1PA выбирает другой IP-адрес и, если надо, повторяет эту операцию до 10 раз.

Примечание Центр выделенных номеров Интернета (IANA, Internet Assigned Numbers Authority) зарезервировал адреса с 169.254.0.0 по 169.254.255.255 для AP1PA. Благодаря этому APIPA назначает адрес, который гарантированно не будет конфликтовать с маршрутизируемыми адресами.

Сгенерировав адрес, компьютер производит на него широковещательную рассылку и, если ответа нет, присвоит адрес себе и будет использовать до тех пор, пока не обнаружит и не получит конфигурационную информацию от сервера DHCP. Это позволяет подключить два компьютера к концентратору ЛВС, перезагрузить их без настройки IP-адресов и использовать TCP/IP для доступа к ЛВС.

Примечание Windows 98 также поддерживает APIPA.

Хотя AP1PA может автоматически присваивать клиентам DHCP IP-адрес, она не генерирует всей информации, обычно поступающей от службы DHCP. Так, APIPA не генерирует адрес шлюза по умолчанию. Соответственно, компьютеры, подключенные к сети с использованием APIPA, могут связываться только с компьютерами той же подсети, имеющими адреса вида 169.254.*x.y*.

Отключение автоматической IP-адресации

По умолчанию функция автоматической IP-адресации включена. Но ее можно отключить, добавив в подраздел HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces*Adapter_GUID* реестра параметр IPAutoconfigurationEnabled и присвоив ему значение 0.

Тип значения параметра IPAutoconfigurationEnabled — REG_DWORD. Чтобы отключить APIPA, задайте этому параметру значение 0. Чтобы включить AP1PA, задайте 1 (значение по умолчанию, используемое при отсутствии в реестре параметра IPAutoconfigurationEnabled).

Устранение неполадок TCP/IP

Несколько утилит в Windows 2000 упрощают решение проблем с TCP/IP.

Утилита	Описание
Ping	Проверяет конфигурацию и тестирует соединение
Arp	Отображает локально определенный IP-адрес в виде физического адреса
Ipconfig	Отображает текущую конфигурацию TCP/IP
Nbtstat	Отображает статистику соединений, использующих NetBIOS поверх TCP/IP
Netstat	Отображает статистику протокола TCP/IP и соединения, использующие этот пакет протоколов
Route	Выводит или изменяет локальную таблицу маршрутизации
Hostname	Выводит имя узла, на котором была сформирована команда
Tracert	Проверяет маршрут к удаленной системе

Проверка возможности соединения с использованием TCP/IP

В Windows 2000 имеется ряд распространенных утилит TCP/IP:

Утилита	Описание
FTP	Обеспечивает двунаправленную передачу файлов между компьютером с Windows 2000 и любым TCP/IP-хостом под управлением FTP Компьютер Windows 2000 Server может выступать и как FTP-клиент, и как FTP-сервер.
Trivial File Transfer Protocol (TFTP)	Обеспечивает двунаправленную передачу файлов между компьютером с Windows 2000 и TCP/IP-хостом под управлением TFTP.
Telnet	Предоставляет TCP/IP-хосту под управлением Telnet эмуляцию терминала., Компьютер с Windows 2000 Server может быть клиентом Telnet.
Remote Copy Protocol (RCP)	Копирует файлы между клиентом и узлом, поддерживающим протокол RCP, например, между компьютером с Windows 2000 и узлом UNIX.
Remote shell (RSH)	Выполняет команды на узла UNIX.
Remote execution (REXEC)	Запускает процесс на удаленном компьютере.
Finger	Возвращает системную информацию с удаленного компьютера, поддерживающего TCP/IP и утилиту finger.

Настроив TCP/IP и перезапустив компьютер, проверьте конфигурацию и соединение с другими узлами и сетями TCP/IP, используя утилиты командной строки ipconfig и ping, что позволит Вам убедиться в корректной работе TCP/IP.

Утилита ipconfig

Служит для проверки конфигурационных параметров узла TCP/IP. Это позволит Вам определить, инициализирована ли конфигурация и есть ли идентичные IP-адреса. Чтобы получить все сведения о конфигурации, запустите ipconfig с параметром /all.

Подсказка Для постепенного вывода информации наберите ipconfig /all | **more**; чтобы перейти к следующему фрагменту, нажмите пробел. Для вывода всех сведений в файл ipconfig. txt наберите **ipconfig /all > ipconfig.txt**. Созданный файл можно просмотреть в любом текстовом *редакторе, поддерживающем* стандарт ASCII, например, в Notepad *(Блокнот)*.

Ниже описаны результаты выполнения команды ipconfig /all:

- если конфигурация была инициализирована, ipconfig выведет IP-адрес, маску подсети и шлюз по умолчанию (если таковой определен);
- в случае существования идентичного IP-адреса ipconfig выведет IP-адрес и маску подсети; при этом маска подсети будет 0.0.0.0;
- если компьютер не может получить от сервера, на котором выполняется служба DHCP, IP-адрес, ipconfig выдаст IP-адрес, выделенный механизмом APTPA.

Утилита ping

Протестировав конфигурацию TCP/IP, с помощью ping проверьте возможность установления связи. Утилита ping — диагностическое средство для проверки конфигураций TCP/IP и выявления сбоев соединений и позволяет проверить доступность и функциональность определенного узла TCP/IP. Для проверки возможности установления соединения используйте синтаксис:

ping *<IP-адрес>*

Совместное использование утилит ipconfig и ping

Совместно применяя ipconfig и ping, можно проверять конфигурацию компьютера и тестировать соединения с маршрутизатором:

1. с помощью ipconfig проверьте, инициализирована ли конфигурация TCP/IP;
2. выполнив команду ping с адресом возвратной петли (127.0.0.1), убедитесь, что стек протоколов TCP/IP корректно установлен и привязан к сетевой плате;
3. выполнив команду ping с IP-адресом локального компьютера, убедитесь, что в сети отсутствует идентичный IP-адрес;
4. выполнив команду ping с IP-адресом шлюза по умолчанию, убедитесь, что шлюз работает и компьютер может взаимодействовать с локальной сетью;
5. выполнив команду ping с IP-адресом удаленного узла, убедитесь, что компьютер может устанавливать соединение через маршрутизатор.

Примечание Обычно, если опрос удаленного узла прошел успешно (п. 5), подразумевается, что при выполнении пп. 1-4 проблем тоже не возникло. В случае неудачи при выполнении п. 5, прежде чем завершить диагностику, попробуйте опросить другой удаленный узел, так как первый узел мог быть отключен.

Упражнение 1: конфигурирование и проверка TCP/IP

С помощью утилит ipconfig и ping Вы проверите конфигурацию TCP/IP на Server01. Затем Вы настроите Server01 для использования статичного IP-адреса и проверите новую конфигурацию. После этого Вы настроите ServerOl для автоматического получения IP-адреса и проверите механизм APIPA. Выполняйте упражнение на Server01.

Внимание! В Вашей сети не должна быть запущена служба **DHCP.** Кроме того, Вам придется назначить IP-адреса, которые могут оказаться недействительными для Вашей сети. Если Ваша сеть входит в более крупную, где используется DHCP, изолируйте свою сеть от нее.

► Задание 1: проверьте конфигурацию TCP/IP

Вы проверите статичную конфигурацию компьютера, используя ipconfig и ping.

1. Зарегистрируйтесь на ServerOl как Administrator с паролем **password**.
2. Откройте окно командной строки.
3. Наберите ipconfig /all | **more** и нажмите клавишу Enter. (Вертикальная линия между словами «all» и «more» является знаком разорванной линии, обычно изображаемым на клавише «V.)

   Утилита Windows 2000 IP Configuration отобразит конфигурацию TCP/IP адаптера(ов), установленного на компьютере,
4. При необходимости нажимайте пробел, пока не увидите заголовок <*тип адаптера*> adapter Local Area Connection (Адаптер <*тип адаптера*> Подключение по локальной сети). Используя значения, отображаемые на экране, заполните пустые поля таблицы (некоторые значения таблицы **Вы** задали ранее, выполняя конфигурационные процедуры в предыдущих упражнениях):

Параметры локального соединения	Значение
Host Name (Имя компьютера)	SERVER01
Primary DNS Suffix (Основной DNS суффикс)	Microsoft.com
DNS Servers (DNS-серверы)	**10.10.10.1**
Description (Описание)	
Physical Address (Физический адрес)	
DHCP Enabled (DHCP разрешен)	No (Нет)
Subnet **Mask** (Маска **подсети)**	255.0.0.0
Default Gateway (Основной шлюз)	

5. Нажимайте клавишу пробела, пока вновь не появится приглашение командной строки.
6. Чтобы убедиться, что для адаптера задан и используется IP-адрес, наберите **ping 127.0.0.1** и затем нажмите Enter.

   Данный IP-адрес называется *адресом возвратной петли* (loop-back address) и применяется для проверки корректной работы стека TCP/IP.

   Если на экран будут выведены результаты, аналогичные приведенным ниже, опрос прошел успешно:

```
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Ping statistics for 127.0,0.1:
Packets; Sent = 4, Received = 4, Lost = 0 <0% loss>,
Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum - Oms, Average = 0ms
```

7. Сверните окно сеанса MS-DOS — оно понадобится в следующих упражнениях.

► Задание 2: настройте TCP/IP для автоматического получения IP-адреса

Вы настроите TCP/IP для автоматического получения IP-адреса. Затем Вы проверите конфигурацию и убедитесь, что механизм APIPA предоставил соответствующую информацию об IP-адресе. Выполняйте упражнение на Server01 и Server02.

1. Раскройте меню Start\Settings (Пуск\Настройка) и выберите Network And Dial-Up Connections (Сеть и удаленный доступ к сети).

   Откроется одноименное окно.
2. Выделите Local Area Connection (Подключение по локальной сети) и в меню File (Файл) выберите команду Properties (Свойства).

   Откроется диалоговое окно Local Area Connection Properties (Подключение по локальной сети — свойства), где показан задействованный сетевой адаптер, а также сетевые компоненты, используемые данным соединением.
3. Щелкните Internet Protocol (TCP/IP) (Протокол Интернета) и убедитесь, что против этого элемента помечен флажок.
4. Щелкните кнопку Properties (Свойства).

   Откроется диалоговое окно Internet Protocol (TCP/IP) Properties (Свойства: Протокол Интернета).
5. Щелкните переключатель Obtain An IP Address Automatically (Получить IP-адрес автоматически).
6. Щелкните переключатель Obtain DNS Server Address Automatically (Получить адрес DNS-сервера автоматически).
7. Щелкните кнопку OK, чтобы закрыть диалоговое окно Internet Protocol (TCP/IP) Properties.
8. Щелкните кнопку OK, чтобы закрыть диалоговое окно Local Area Connection Properties.
9. Сверните окно Network And Dial-Up Connections.
10. В командной строке наберите **ipconfig** /all | more и нажмите клавишу Enter.
11. Нажимая клавишу пробела, найдите текущие параметры для *<тип адаптера>* adapter Local Area Connection и заполните таблицу (некоторые поля уже заполнены):

Параметр	Значение
Autoconfiguration Enabled	Yes
IP Address	
Subnet Mask	
DHCP Enabled	Yes
Default Gateway	None – requires manual configuration or DHCP
DNS Servers	None - requires manual configuration or DHCP

Заметьте: IP-адрес и маска подсети, назначенные APIPA, отличаются от значений, указанных вручную. Кроме того, IP-адрес помечен как Autoconfiguration IP Address, и используется DHCP. Служба DHCP используется, так как Вы указали, что IP-адрес должен назначаться автоматически.

12. Нажимая при необходимости клавишу пробела, вернитесь к командной строке.
13. Чтобы убедиться, что TCP/IP функционирует и привязан к Вашему адаптеру, наберите ping 127.0.0.1 и нажмите клавишу Enter.

    Если TCP/IP привязан к адаптеру, в результате внутренней проверки по адресу возвратной петли на экран будет выведено 4 отклика.
14. Закройте окно командной строки, а затем — окно Network And Dial-Up Connections.

Резюме

Разработанная Microsoft реализация протокола TCP/IP позволяет создавать сети и обеспечивает связь между компьютерами. Стек протоколов TCP/IP включает 4 уровня: сетевого интерфейса, Интернета, транспортный и прикладной. По умолчанию клиент с Windows 2000 автоматически получает сведения о конфигурации TCP/IP от службы DHCP; однако некоторые компьютеры требуют выделения статичного IP-адреса. Для каждого сетевого адаптера, использующего TC P/IP, надо определить IP-адрес, маску подсети и шлюз по умолчанию. Реализация TCP/IP в Windows 2000 также поддерживает механизм APIPA (автоматическая закрытая IP-адресация), обеспечивающий автоматическое присвоение IP-адресов простым ЛВС-конфигурациям. APIPA позволяет выделять IP-адреса без применения механизма статичных IP-адресов или установки службы DHCP. Windows 2000 включает средства для устранения неполадок TCP/IP и проверки возможности установления связи: ping, ipconfig, FTP и Telnet.

Занятие 3. Служба DHCP

Служба DHCP собирает и выделяет конфигурационную информацию TCP/IP, автоматически присваивая DHCP-клиентам IP-адреса и иные данные TCP/IP. Внедрение службы DHCP может разрешить массу проблем, связанных с ручной настройкой TCP/IP. Вы узнаете, как установить и настроить службу DHCP. Кроме того, мы рассмотрим процесс аренды DHCP.

Изучив материал этого занятия, Вы сможете:

- ✓ установить службу DHCP;
- ✓ определить область службы DHCP, настроить диапазон адресов и зафиксировать границы применения DHCP;
- ✓ выполнить резервное копирование и восстановить базу данных DHCP.

Продолжительность занятия — около 70 минут.

Введение в DHCP

DHCP представляет стандарт стека протоколов TCP/IP, упрощающий обслуживание IP-конфигурации. DHCP — это расширение протокола Bootstrap Protocol (BOOTP), основанного на протоколе UDP/IP. BOOTP позволяет загружающемуся узлу динамически конфигурировать себя.

При каждом запуске клиент DHCP запрашивает у сервера DHCP;

- IP-адрес;
- маску подсети;
- дополнительные значения, например, адрес шлюза по умолчанию, адрес сервера DNS или WINS.

Получив запрос на IP-адрес, сервер DHCP выбирает информацию об IP-адресе из пула адресов, определенных в его БД, и предлагает эти данные клиенту DHCP. Если клиент принимает предложение, сервер DHCP выделяет ему на определенный срок IP-адрес,

Ручная и автоматическая настройка TCP/IP

Чтобы понять преимущества использования службы DHCP для настройки TCP/I P на клиентских компьютерах, сравним ручную настройку TCP/IP и автоматическую.

Ручная настройка TCP/IP	Настройка TCP/IP с использованием DHCP
Пользователи могут выбрать IP-адрес произвольно, а не получать его у сетевого администратора. Применение некорректных адресов может вызвать сбои в работе сети, которые сложно отследить.	Для настройки TCP/IP пользователям вообще не надо обращаться к сетевому администратору за сведениями об IP-адресе. Служба DHCP предоставляет всем клиентам DHCP нужную конфигурационную информацию.
Поскольку IP-адрес, маски подсети и шлюз по умолчанию задаются вручную, это может привести к разным проблемам — от проблем со связью, если был неправильно указан шлюз по умолчанию или маска подсети, до идентичных IP-адресов	Действительные сведения об IP-адресе гарантируют корректность конфигурации, избавляя Вас от большинства проблем с сетью, источник которых трудно определить.

(окончание)

Ручная настройка TCP/IP	Настройка TCP/IP с использованием DHCP
При частом перемещении компьютеров из одной подсети в другую усложняется администрирование. Например, чтобы клиент мог устанавливать связь из нового места, Вам придется изменить его IP-адрес и шлюз по умолчанию.	Наличие в каждой подсети серверов DHCP полностью избавляет от проблем с ручной перенастройкой IP-адресов, масок подсети и шлюзов по умолчанию, возникающих при перемещении компьютера из одной подсети в другую. Помните:] сервер DHCP способен выделять IP-адреса нескольким сетям.

Аренда DHCP

Служба DHCP предоставляет клиентским компьютерам сведения об IP-адресе. Этот процесс называется *арендой DHCP* и имеет место в одном из следующих случаев:

- на клиенте DHCP впервые инициализирован пакет протоколов TCP/IP;
- клиент запросил определенный IP-адрес и получил отказ, возможно, в связи с тем, что сервер DHCP отозвал предоставленный адрес;
- клиент, ранее арендовавший IP-адрес и освободивший его, запросил новый адрес; выделенный DHCP-сервером IP-адрес можно освободить вручную, запустив в командной строке утилиту **ipconfig** с параметром /release.

Выделение IP-адреса клиенту DHCP производится сервером DHCP в четыре этапа: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST и DHCPACK (рис. 9-5).

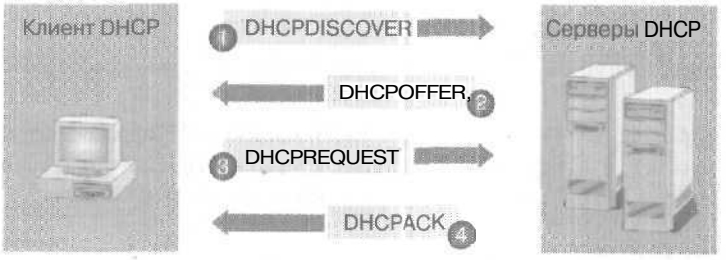


Рис. 9-5. Выделение IP-адреса с использованием DHCP

DHCPDISCOVER

Это первый этап выделения IP-адреса с использованием DHCP. Сначала клиент инициализирует ограниченную версию TCP/IP и производит широковещательную рассылку сообщения DHCPDISCOVER, запрашивая местоположение DHCP-сервера и сведения об IP-адресе. Поскольку клиент не знает IP-адреса сервера DHCP, в качестве исходного адреса применяется 0.0.0.0, а конечного — 255.255.255.255. Сообщение DHCPDISCOVER содержит аппаратный адрес клиента и имя компьютера, по которому сервер DHCP может определить клиент, отославший запрос.

DHCPOFFER

Это второй этап. Все серверы DHCP, получившие запрос на выделение IP-адреса и имеющие правильную клиентскую конфигурацию, производят широковещательную рассылку сообщения DHCPOFFER, включающего:

- аппаратный адрес клиента;
- предлагаемый IP-адрес;

- маску подсети;
- период аренды адреса;
- идентификатор сервера (IP-адрес предлагающего сервера DHCP).

Широковещание используется, поскольку у клиента еще нет IP-адреса. Клиент DHCP выбирает IP-адрес из первого полученного предложения. Сервер DHCP, предлагающий IP-адрес, резервирует его, чтобы не предложить другому клиенту.

DHCPREQUEST

Третий этап наступает после того, как клиент примет сообщение DHCPOFFER от хотя бы одного сервера DHCP и выберет IP-адрес. Клиент производит широковещательную рассылку сообщения DHCPREQUEST всем серверам DHCP, сообщая им, что он уже принял предложение. DHCPREQUEST включает идентификатор сервера (IP-адрес), предложение которого было принято клиентом. Затем остальные серверы DHCP отзывают свои предложения и сохраняют IP-адреса для следующих запросов.

DHCPACK

Последний этап процесса выделения IP-адреса с использованием DHCP наступает после того, как сервер DHCP, чье предложение было принято, выполнит широковещательную рассылку положительного подтверждения клиенту. Подтверждение распространяется в форме сообщения DHCPACK, содержащего действительный IP-адрес и, возможно, другую конфигурационную информацию.

При получении клиентом подтверждения выполняется полная инициализация TCP/IP, и клиент считается привязанным клиентом DHCP. После этого клиент может использовать для связи TCP/IP.

DHCPNACK

В случае неудачи на этапе DHCPREQUEST сервер DHCP производит широковещательную рассылку отрицательного подтверждения (DHCPNACK). Это происходит в одном из случаев:

- клиент пытается получить свой предыдущий IP-адрес, который уже недоступен;
- IP-адрес неверен, поскольку компьютер был перемещен в другую подсеть.

Получив отрицательное подтверждение, клиент возобновляет процесс получения IP-адреса с использованием DHCP.

Примечание Если в компьютере несколько сетевых адаптеров, привязанных к TCP/IP, процесс DHCP осуществляется отдельно для каждого. Служба DHCP выделяет каждому адаптеру уникальный и действительный IP-адрес.

Продление аренды и освобождение IP-адреса

По прошествии половины периода, на который был выделен IP-адрес, клиенты DHCP пытаются продлить его аренду. Для этого клиент посылает сообщение DHCPREQUEST прямо выделившему адрес серверу DHCP, Если он доступен, то продлевает аренду и отсылает клиенту сообщение DHCPACK с новым временем аренды и обновленными параметрами конфигурации. Получив подтверждение, клиент обновляет свою конфигурацию.

Примечание При каждом перезапуске клиент DHCP пытается получить у исходного сервера DHCP свой старый IP-адрес. Если эта попытка окажется неудачной и время аренды еще не кончилось, клиент DHCP будет использовать старый IP-адрес до следующей попытки продления аренды.

Если по прошествии половины времени аренды клиент DHCP не сможет продлить ее на исходном сервере DHCP, по истечении 87.5% времени аренды клиент начнет широковещательную рассылку пакета DHCPREQUEST для связи с любым доступным сервером DHCP. Сервер DHCP может ответить либо сообщением DHCPACK (продление аренды), либо DHCPNACK (принудительная инициализация клиента и получение им другого IP-адреса).

По истечении срока аренды или получив сообщение DHCPNACK, клиент DHCP должен сразу прекратить использование занятого IP-адреса. Затем клиент возобновляет процесс аренды DHCP для получения нового IP-адреса.

Продление аренды IP-адреса с помощью ipconfig

Чтобы отослать серверу DHCP сообщение DCHPREQUEST и получить обновленные параметры и период аренды, запустите в командной строке ipconfig с ключом /renew. Если сервер DHCP недоступен, клиент продолжит использовать текущие параметры конфигурации, предоставленные DHCP.

Освобождение IP-адреса с помощью ipconfig

Чтобы отослать серверу DHCP сообщение DHCPRELEASE и освободить занимаемый клиентом DHCP IP-адрес, запустите в командной строке ipconfig с ключом /release. Это полезно, если Вы перемещаете клиентский компьютер в другую сеть и ему не нужен старый IP-адрес. После выполнения этой команды связь с клиентом с применением TCP/IP прекращается.

При отключении системы клиенты DHCP компании Microsoft не отсылают сообщений DHCPRELEASE. Если клиент остается отключенным на период аренды (и аренда не продляется), по истечении срока аренды сервер DHCP может присвоить IP-адрес клиента другому компьютеру. Если клиент не отсылал сообщение DHCPRELEASE, его шансы на получение в процессе инициализации старого IP-адреса значительно повышаются.

Примечание О реализации DHCP в Windows 2000 см. также документ \chapt09\articles\DHCP2000.doc на прилагаемом компакт-диске.

Установка и настройка службы DHCP

Для внедрения DHCP надо установить и настроить службу DHCP минимум на одном компьютере с Windows 2000 Server в сети TCP/IP. Компьютер можно настроить как контроллер домена или автономный сервер. Кроме того, для корректной работы DHCP надо вручную сконфигурировать параметры TCP/IP для данного сервера и настроить клиенты для получения динамических адресов.

Требования к серверу DHCP

Сервер DHCP должен быть установлен на компьютере с Windows 2000, который должен иметь:

- статичный IP-адрес, маску подсети, шлюз по умолчанию (при необходимости) и иные параметры TCP/IP; сервер DHCP не может быть клиентом DHCP;
- службу DHCP;
- активную область DHCP, т. е. диапазон IP-адресов, которые сервер может присваивать клиентам; после определения области ее надо активизировать;
- авторизацию: сервер DHCPдолжен быть авторизован службой Active Directory.

Требования к клиентам DHCP

Клиент DHCP должен устанавливаться на компьютере с поддержкой DHCP, работающем под управлением одной из ОС:

- Windows 2000;
- Windows NT Server, начиная с версии 3.51;
- Windows NT Workstation, начиная с версии 3.51;
- Windows98;
- Windows 95;
- Windows for Workgroups 3.11, использующей Microsoft TCP/IP-32;
- Microsoft Network Client 3.0 for Microsoft MS-DOS с драйвером TCP/IP реального режима;
- LAN Manager version 2.2c for MS-DOS (LAN Manager2.2c for OS/2 не поддерживается).

Установка службы DHCP

Первый этап реализации DHCP — установка службы DHCP. Прежде чем установить службу DHCP, для привязанного к TCP/IP сетевого адаптера сервера надо указать статичный IP-адрес, маску подсети и шлюз по умолчанию.

Для установки службы DHCP используйте утилиту Add/Remove Programs из Control Panel. Служба DHCP автоматически активизируется в ходе установки; для связи с клиентами DHCP она должна быть запущена.

Оснастка DHCP

Для конфигурации и управления DHCP можно вызвать оснастку DHCP (рис. 9-6), которая отображает подробные сведения об областях и параметрах DHCP. Эта оснастка позволяет создавать и изменять области, просматривать выделенные адреса, резервировать и изменять зарезервированные, а также задавать параметры сервера, области и зарезервированных адресов.

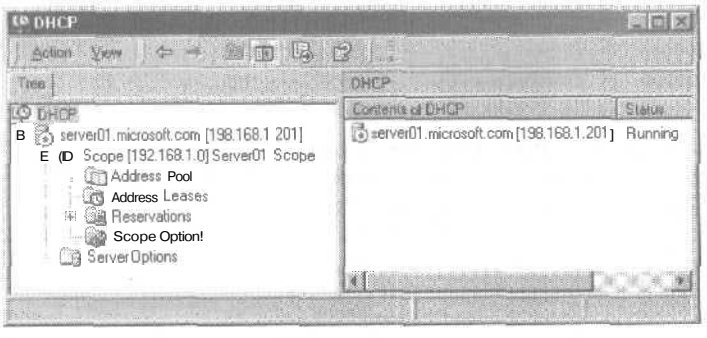


Рис. 9-6. Оснастка DHCP

Оснастку DHCP можно запустить из консоли управления (MMC) или из оснастки Computer Management (Управление компьютером). Для установки оснастки DHCP запустите файл Adminpak.msi или установите службу DHCP. При отсутствии службы DHCP эта оснастка применяется для управления удаленными серверами, реализующими службу DHCP.

Определение области DHCP

Прежде чем сервер DHCP сможет предоставить клиентам DHCP IP-адреса, надо определить область DHCP — пул действительных IP-адресов, которые могут быть выделены клиентам DHCP.

Создавая область DHCP, помните:

- для каждого сервера DHCP надо определить не менее одной области;
- из области следует исключить статичные IP-адреса;
- для централизации администрирования и выделения IP-адресов, специфичных для конкретной сети, на сервере DCHP можно определить несколько областей; подсети можно присвоить лишь одну область;
- серверы DHCP не обмениваются информацией об областях, поэтому, создавая области на нескольких серверах DHCP, убедитесь, что в этих областях нет пересекающихся IP-адресов — это поможет избежать проблем с идентичными IP-адресами.

Определить область позволяет оснастка DHCP. Вот некоторые параметры, указываемые при создании области:

Параметр	Описание
Name (Имя)	Имя области.
Description (Описание)	Необязательное описание области.
Start **IP Address** (**Начальный** IP-адрес)	Начальный IP-адрес диапазона адресов, которые могут клиенту DHCP из выделяться данной области.
End IP Address (Конечный IP-адрес)	Конечный IP-адрес диапазона адресов, которые могут выделяться клиенту DHCP из данной области.
Subnet Mask (Маска подсети)	Маска подсети, присваиваемая клиентам DHCP, Вы можете определить маску подсети как последовательность бит или как действительную маску подсети.
Start IP Address для диапазона исключений	Начальный IP-адрес диапазона, исключаемого из пула адресов. Адреса этого диапазона не могут выделяться клиентам DHCP. Данную функцию следует применять, если Вы выделили статичные IP-адреса компьютерам — не клиентам DHCP. (Определять исключаемый диапазон необязательно.)
End IP Address для диапазона исключений	Конечный IP-адрес диапазона, исключаемого из пула адресов. Адреса этого диапазона не могут выделяться клиентам DHCP. Данную функцию следует применять, если Вы выделили статичные IP-адреса компьютерам — не клиентам DHCP. (Определять исключаемый диапазон необязательно.)
Lease Duration (Срок действия аренды адреса)	Продолжительность аренды IP-адреса в днях, часах и минутах. По истечении срока аренды клиент DHCP должен продлить ее.

Определив области, активизируйте их. чтобы их можно было использовать для выделения IP-адресов: выделив требуемую область, выберите в меню Action (Действие) команду Activate (Активизировать).

Примечание Для задания новой маски подсети или диапазона IP-адресов область надо удалить и повторно создать.

Настройка области DHCP

Определив область, можно настроить параметры клиентов DHCP. Есть три уровня параметров области: сервера, области и клиента.

Параметры сервера

Доступны всем клиентам DHCP. Эти параметры следует использовать, если всем клиентам во всех подсетях нужна одинаковая конфигурационная информация. Например, можно настроить все клиенты для обращения к одному WINS-серверу. Параметры сервера применяются, если не заданы параметры области или параметры клиента. Для настройки параметров сервера щелкните узел Server Options (Параметры сервера) и в меню Action (Действие) выберите команду Configure Options (Настроить параметры).

Параметры области

Доступны лишь клиентам, арендующим адреса из определенной области. Например, если для каждой подсети Вы определили разные области, можно задать и уникальные адреса шлюзов по умолчанию. Параметры области перенастраивают параметры сервера. Чтобы задать параметры определенной области, щелкните узел Scope Options (Параметры области) и в меню Action (Действие) выберите команду Configure Options (Настроить параметры).

Параметры клиента

Доступны определенным клиентам, зарезервировавшим IP-адреса на сервере DHCP, и переопределяют параметры сервера и области. Для настройки параметров клиента выделите требуемый зарезервированный адрес и в меню Action (Действие) выберите команду Configure Options (Настроить параметры).

Настройка параметров DHCP

Ниже описываются некоторые параметры, применяемые при настройке сервера DHCP, области или зарезервированного адреса. В диалоговом окне свойств сервера, области или зарезервированного адреса выводятся все параметры, поддерживаемые Microsoft DHCP.

Параметр	Описание
044 WINS/NBNS Servers (044 WINS/NBNS-серверы)	IP-адрес WINS/NBNS-сервера, доступного клиентам. Адрес WINS-сервера, вручную заданный на клиентской системе. переопределит соответствующие параметры, устанавливаемые DHCP.
003 Router (003 Маршрутизатор)	IP-адрес маршрутизатора, например, адрес шлюза по умолчанию. Шлюз по умолчанию, локально определенный на клиенте, имеет преимущество над соответствующим параметром DHCP Чтобы убедиться, что информация о маршрутизаторе отослана на клиентский компьютер, проверьте на клиентской системе поле Default Gateway (Шлюз по умолчанию) (рис. 9-4): оно должно быть пустым.
006 DNS Servers (DNS-серверы)	IP-адрес сервера DNS. DNS, локально определенная на клиенте, имеет преимущество над соответствующим параметром DHCP. Убедитесь, что на клиенте установлен переключатель Obtain DNS Server Address Automatically (Получить адрес DNS-сервера автоматически) (рис. 9-4).
015 DNS Domain Name (015 DNS-имя домена)	Доменное имя DNS для разрешения имен клиентов.

(окончание)

Параметр	Описание
046 WINS/NBT Node Type (046 Тип узла WINS/NBT)	Тип разрешения имен NetBIOS поверх TCP/IP, используемого клиентом. Возможные значения: 1=B-node (широковещательный), 2=P-node (одноранговый), 4 = M-node (смешанный) и 8=H-node (гибридный).
047 NetBIOS Scope ID (047 Код области NetBIOS)	Локальный идентификатор области, используемый NetBIOS поверх TCP/IP. NetBIOS поверх TCP/IP устанавливает связь лишь с хостами NetBIOS, использующими идентичный идентификатор области.

Ниже описаны типы значений, используемых при настройке параметров DHCP:

Тип значения	Описание
IP Address (IP-адрес)	IP-адрес сервера, например, 003 Routers
Long (Длинное целое)	32-разрядное численное значение, например, 035 ARP Cache Timeout
String Value (Строковое значение)	Строковое значение, например, 035 Domain Name
Word (Слово)	16-разрядное числовое значение, указывающее размеры определенных блоков, например, 022 Max DG Reassembly Size
Byte (Байт)	Численное значение, состоящее из 1 байта, например, 046 WINS/NBT Node Type
Binary (Двоичные данные)	Двоичное значение, например, 043 Vendor Specific Information

Резервирование IP-адреса

Для некоторых клиентов DHCP важно, чтобы по окончании срока аренды им был выделен тот же IP-адрес. Например, клиенты, реализующие службы сервера TCP/IP, могут использовать статичные IP-адреса, упрощающие идентификацию этих машин для остальных компьютеров сети. Службу DHCP можно настроить так, чтобы клиентам, реализующим службы сервера, всегда выделялись одни и те же адреса. Это называется *резервированием IP-адреса* и осуществляется из диалогового окна New Reservation (Создать резервирование) (рис. 9-7).

Клиенту, использующему статичное определение имен хоста, может потребоваться, чтобы конфигурация его IP-адреса хранилась на сервере. Например, если сервер с именем хоста SRV187 находится в сети, включающей клиентов, которые осуществляют разрешение имен с применением статичного файла HOSTS или LMHOSTS, для SRV187 надо зарезервировать IP-адрес. После этого он будет получать с сервера DHCP один и тот же IP-адрес. Клиенты без поддержки WINS для разрешения NetBIOS-имен компьютеров должны применять файл LMHOSTS, клиенты без поддержки DNS для разрешения IP-имен хостов — файл HOSTS. Поскольку файлы LMHOSTS и HOSTS представляют собой статичные файлы, содержащие привязку имен к IP-адресам, в случае смены IP-адреса сервера SRV187 при разрешении имен произойдет ошибка.

Чтобы зарезервировать для клиента IP-адрес, щелкните подузел Reservations (Резервирование) требуемого узла области *к* выберите в меню Action (Действие) команду New Reservation (Создать резервирование). Убедитесь, что Вы правильно указали IP- и MAC-адрес. Неверно заданный MAC-адрес не будет соответствовать значению, отсылаемому

клиентом DHCP, и служба DHCP вместо зарезервированного IP-адреса выделит этому клиенту один из доступных адресов. Если Вы заменили на клиенте сетевую плату, не забудьте указать новый MAC-адрес в параметрах зарезервированного IP-адреса.

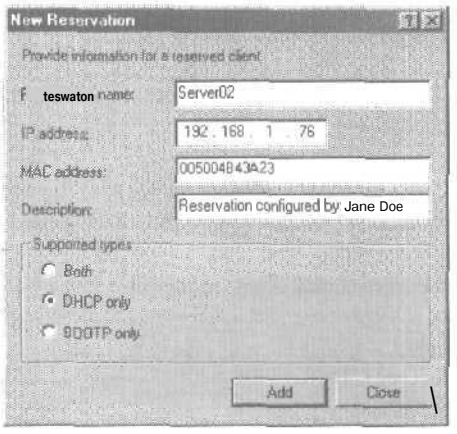


Рис. 9-7. **Резервирование IP-адреса в диалоговом окне** New **Reservation (Создать резервирование)**

Авторизация сервера DHCP

Прежде чем начать выделение IP-адресов, сервер DHCP должен быть авторизован службой каталогов Active Directory. Авторизация — это одна из мер безопасности, гарантирующая, что в сети работают лишь проверенные серверы DHCP. Для авторизации сервера DHCP выделите в дереве оснастки DHCP домен, а затем в меню Action (Действие) выберите команду Authorize (Авторизовать).

Упражнение 2: установка и настройка службы DHCP

Вы установите и настроите службу DHCP на Server01. Затем Вы определите область и зададите для нее небольшой диапазон. Как и в упражнении 1, убедитесь, что ServerOl находится в изолированной сети. Это поможет избежать конфликтов, связанных с IP-адресами. Некоторые этапы следует выполнять на Server01, а другие — на *Server02.*

► Задание 1: настройте параметры TCP/IP на ServerOl для использования статичного IP-адреса

Вы настроите ServerOl для использования статичного IP-адреса — это необходимое условие для установки службы DHCP.

1. Зарегистрируйтесь на ServerOl как Administrator с паролем password.
2. Раскройте меню Start\Settings (Пуск\Настройка) и щелкните ярлык Network And Dial-up Connections (Сеть и удаленный доступ к сети).

   Откроется одноименное окно.
3. Выделите Local Area Connection (Подключение по локальной сети) и в меню File (Файл) выберите команду Properties (Свойства).

   Откроется диалоговое окно свойств локального подключения, где показан задействованный сетевой адаптер, а также сетевые компоненты, используемые данным соединением.

4. Щелкните Internet Protocol (TCP/IP) (Протокол Интернета) и убедитесь, что против этого элемента установлен флажок.
5. Щелкните кнопку Properties (Свойства).

   Откроется диалоговое окно свойств TCP/IP.
6. Щелкните переключатель Use The Following IP Address (Использовать следующий IP-адрес).
7. В поле IP address (IP-адрес) введите 192.168.1.201, нажмите клавишу Tab и убедитесь, что в поле Subnet mask (Маска подсети) указано 255.255.255.0.
8. Щелкните кнопку OK.

   Появится сообщение Microsoft TCP/IP о том, что список серверов DNS пуст и, поскольку на компьютере установлена DNS, будет использоваться локальный IP-адрес.
9. Щелкните кнопку OK.
10. Щелкните кнопку OK, чтобы закрыть диалоговое окно Local Area Connection Properties (Подключение по локальной сети).
11. Сверните окно Network And Dial-Up Connections.

► Задание 2: определите физический адрес компьютера

Вы определите физический адрес Server02. Он потребуется Вам на одном из следующих этапов для резервирования IP-адреса.

1. Убедитесь, что Server02 подключен к той же изолированной сети, что и Server01. Затем зарегистрируйтесь на Server02 как Administrator с паролем **password.**
2. Чтобы определить физический адрес адаптера на Server02, откройте сеанс MS-DOS и в командной строке введите **ipconfig /all | more.**

Примечание Допустим, для Server02 задан действительный IP-адрес, доступный с ServerOl. Тогда MAC-адрес сетевого адаптера, установленного на Server02, можно получить с Server01. Для этого выполните на ServerOl команду ping *<IP-адрес_Server02>*, затем введите в командной строке arp -a и нажмите клавишу Enter, чтобы определить MAC-адрес сетевого адаптера Server02.

---

3. Запишите физический адрес Server02, показанный в выведенной на экран строке.

   Физический адрес — это аппаратный или MAC-адрес. Физический адрес «вшит» в сетевой адаптер и выглядит следующим образом: 00-50-04-B4-3A-23.
4. Сверните окно командной строки на Server02.

► Задание 3: установите службу DHCP

Вы установите службу DHCP на Server01.

1. На ServerOl раскройте меню Start\Programs (Пуск\Программы) и выберите Administrative Tools (Администрирование).

   Заметьте: в списке служебных программ имеется DHCP. Оснастка DHCP установлена, потому что в одном из предыдущих упражнений Вы установили файл Adminpak.msi. Однако присутствует лишь оснастка; служба DHCP на ServerOl не установлена,
2. В меню Start\Settings (Пуск\Настройка) щелкните ярлык Control Panel.
3. Дважды щелкните значок Add/Remove Programs.

   Откроется одноименное окно.
4. Щелкните кнопку Add/Remove Windows Components (Установка и удаление компонентов Windows).
5. В перечне компонентов щелкните пункт Networking Services (Сетевые службы), но не трогайте флажок напротив него.

Примечание Флажок Networking Services должен быть установлен, поскольку на компьютере Server01 уже есть некоторые службы для работы с сетью.

6. Щелкните кнопку Details (Состав).
   Откроется диалоговое окно Networking Services (Сетевые службы).
   В списке компонентов пометьте Dynamic Host Configuration Protocol (DHCP).
7. Щелкните кнопку OK.
8. Щелкните кнопку Next (Далее).
   В соответствующие папки ОС будут скопированы файлы службы DHCP. Откроется окно мастера Completing The Windows Components Wizard (Завершение работы мастера компонентов Windows).
9. Щелкните кнопку Finish (Готово).
10. Закройте окно Add/Remove Programs .
11. Закройте окно Control Panel.

▶ Задание 4: определите и настройте область DHCP

Вы определите и настроите на ServerOl область DHCP.

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и выберите DHCP.
   Откроется оснастка DHCP.
2. Разверните окно оснастки DHCP.
3. В дереве консоли дважды щелкните узел server01.microsoft.com **[192.168.1.201].**
4. В меню Action выберите команду New Scope (Создать область).
   Откроется окно мастера создания области.
5. Щелкните кнопку Next (Далее).
   Откроется окно Scope Name (Имя области).
6. В поле Name (Имя) введите **ServerOl** Scope.
7. В поле Description (Описание) введите Training **network** и щелкните кнопку Next (Далее).
   Откроется окно IP Address Range (Диапазон адресов).
8. В поле Start IP Address (Начальный IP-адрес) введите **192.168.1.70,** а в поле End IP Address (Конечный IP-адрес) - **192.168.1.90.**
   Заметьте: маска указана как стандартный адрес класса С (255.255.255.0), и используются 24 разряда. Все биты первых 3 октетов равны 1.
9. Щелкните кнопку Next (Далее).
   Откроется окно Add Exclusions (Добавление исключений).
10. В поле Start IP Address (Начальный IP-адрес) введите **192.168.1.76,** а в поле End **IP** Address (Конечный IP-адрес) - **192.168.1.80.**
11. Щелкните кнопку Add (Добавить).
    Заметьте: значения 192.168.1,76 — 192.168.1.80 отображаются в списке Excluded Addresses (Исключенный диапазон адресов).
12. Щелкните кнопку Next (Далее).
    Откроется окно Lease Duration (Срок действия аренды адреса). Заметьте, что по умолчанию период аренды IP-адреса равен 8 дням.
13. Щелкните кнопку Next (Далее), чтобы принять период аренды по умолчанию.
    Откроется окно Configure DHCP Options (Настройка параметров DHCP), где Вам будет предложено настроить основные параметры DHCP.

14. Щелкните переключатель No, I Will Configure These Options Later (Нет, настроить эти параметры позже), а затем — кнопку Next.

    Откроется окно Completing The New Scope Wizard (Завершение работы мастера создания области).

15. Изучите представленные инструкции, и затем щелкните кнопку Finish (Готово).

    В оснастке DHCP появится значок, представляющий новую область. В данный момент она отключена. Вы активизируете эту область потом.

► Задание 5: добавьте зарезервированный IP-адрес в область DHCP

Вы зарезервируете IP-адрес, используя физический адрес Server02, полученный на втором этапе.

1. В дереве оснастки DHCP на Server01 щелкните узел Scope [192.168.1.0] Server01 Scope (Область (192.168.1.0] ServerOl Scope).

   В правой панели будет выведено содержимое области.

2. В дереве консоли щелкните узел Reservations (Резервирование) и прочитайте сообщение в правой панели.
3. В меню Action (Действие) выберите команду New Reservation (Создать резервирование).

   Откроется одноименное диалоговое окно.

4. В поле Reservation Name (Имя клиента) введите **Server02**.
5. Заметьте: первые 3 октета поля IP Address (IP-адрес) уже заполнены. В четвертом октете введите 76. IP-адрес должен выглядеть следующим образом: 192.168.1.76.
6. В поле MAC Address (MAC-адрес) введите физический адрес, полученный при выполнении второго этапа. Дефисы вводить не следует.

   Например, физический адрес 00-50-04-B4-3A-23 надо ввести как 005004B43A23.

7. В поле Description (Описание) введите **Reservation made by: <*Ваше имя*>.**

   Данный зарезервированный IP-адрес могут использовать клиенты DHCP, клиенты BOOTP или оба типа клиентов сразу. Клиентом BOOTP может устройство, например, унаследованный терминал или маршрутизатор. На запросы таких клиентов отвечает сервер DHCP и при необходимости передает им дополнительную конфигурационную информацию. Кроме того, поддерживаются динамические области BOOTP (Dynamic BOOTP scopes). Подробнее о параметрах конфигурации см. раздел «Supporting BOOTP Clients» справочной системы DHCP.

8. В группе Supported types (Поддерживаемые типы) щелкните переключатель DHCP Only (Только DHCP) и щелкните кнопку Add (Добавить).

   Откроется новое диалоговое окно New Reservation (Создать резервирование).

9. Щелкните кнопку Close (Закрыть).
10. Заметьте: на правой панели появился зарезервированный IP-адрес.
11. В дереве консоли щелкните узел Scope [192.168.1.0] Server01 Scope (Область [192.168.1.0] ServerOl Scope).
12. В меню Action выберите команду Activate (Активизировать).

    Красная стрелка справа от имени области исчезнет. Заметьте также, что справа от узла server01.microsoft.com [192.168.1.201] по-прежнему отображается направленная вниз стрелка.

13. В дереве консоли щелкните узел server01.microsoft.com [192.168.1.201].
14. Из меню Action выберите команду Authorize (Авторизовать), чтобы авторизовать данный сервер DHCP в хранилище Active Directory.
15. Нажмите клавишу F5, чтобы обновить окно оснастки.

После авторизации службы DHCP справа от узла server01.microsoft.com [192.168.1.201] появится направленная вверх зеленая стрелка.

► Задание 6: настройте параметры области

Вы настроите DHCP так, чтобы при регистрации клиенту DHCP пересылались имя предпочитаемого сервера DNS и доменное имя DNS. Это аналогично настройке параметров сервера, используемых всеми подключенными к нему клиентами, и настройке параметров отдельных клиентов,

1. В дереве консоли раскройте узел server01.microsoft.com [192.168.1.201], подузел Scope [192.168.1.0] Server Scope и щелкните папку Scope Options (Параметры области).
2. В меню Action (Действие) выберите команду Configure Options (Настроить параметры).

   Откроется диалоговое окно Scope Options (Область — параметры).
3. Пометьте флажок 006 DNS Servers (006 DNS-серверы).

   Станут доступными параметры из группы Data Entry (Запись данных).
4. В поле Server Name (Имя сервера) введите **Server01** и щелкните кнопку Resolve (Сопоставить).

   В поле IP Address (IP-адрес) появится адрес 198.168.1.201.
5. Щелкните кнопку Add (Добавить).
6. В списке Available Options (Доступный параметр) пометьте флажком параметр 015 DNS Domain Name (015 DNS-имя домена).
7. В поле String value (Строковое значение) введите microsoft.com и щелкните OK.

   Клиентам DHCP данной области будет передана информация DNS.
8. Не закрывайте оснастку DHCP — она понадобится Вам на следующем этапе.

► Задание 7: проверьте работу службы DHCP

Вы протестируете работу службы DHCP и убедитесь, что на Server02 была передана информация о резервировавшемся для него IP-адресе и этот адрес отображается на ServerOl.

1. На Server02 убедитесь, что в диалоговом окне Internet Protocol (TCP/IP) Properties выбраны переключатели Obtain An IP Address Automatically (Получить IP-адрес автоматически) и Obtain DNS Server Address Automatically (Получить адрес DNS-сервера автоматически).

   Если Вы забыли, как сделать это, вернитесь к упражнению 1.
2. На Server02 восстановите окно командной строки, наберите **ipconfig** /renew и нажмите клавишу Enter.

   Через некоторое Server02 будет присвоен IP-адрес 192.168.1.76.
3. В командной строке введите **ipconfig / all | more** и нажмите Enter.

   Заметьте: на клиент передана информация DHCP. Вы увидите присвоенный сервером DHCP IP-адрес, маску подсети, адрес сервера DNS и доменное имя DNS. Кроме того, клиенту обычно отсылаются дополнительные сведения, например, адрес шлюза по умолчанию.
4. Чтобы проверить связь между Server02 и Server01, в командной строке на Server02 введите ping ServerOl,

   Имя сервера разрешено как server01.microsoft.com и IP-адрес сервера. Такое разрешение имени возможно, поскольку ServerOl переслал компьютеру Server02 с информацией DHCP данные DNS.
5. На ServerOl в дереве оснастки DHCP щелкните папку Addresses Leases (Арендованные адреса).

Заметьте: компьютеру server02.microsoft.com присвоен IP-адрес 192.168.1.76. Кроме того, срок окончания аренды адреса [поле Lease Expiration (Истечение срока аренды)] указан как Reservation (Active) [Резервирование (активное)], так как период аренды зарезервированного адреса неограничен. Для клиента DHCP, IP-адрес которого не зарезервирован, в поле Lease Expiration указаны дата и время окончания срока аренды.

6. Закройте оснастку DHCP на Server01 и окно командной строки на Server02.

Резервное копирование и восстановление базы данных DHCP

Чтобы задать периодичность резервного копирования базы данных DHCP, отредактируйте реестр Windows 2000. Кроме того, БД DHCP можно восстановить вручную, отредактировав реестр.

Резервное копирование БД DHCP

По умолчанию Windows 2000 осуществляет резервное копирование БД DHCP каждые 60 минут. Резервные копии БД DHCP помешаются в папку %systemroot%\System32\Dhcp\Backup\Jet\new.

Чтобы изменить интервал между операциями резервного копирования, отредактируйте значение параметра BackupInterval в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

Восстановление БД DHCP

Поврежденная БД DHCP по умолчанию автоматически восстанавливается при перезапуске службы DHCP, но ее можно восстановить и вручную. Для этого отредактируйте реестр, измените значение параметра RestoreFlag на 1 и перезапустите службу DHCP. Параметр RestoreFlag находится в разделе реестра HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

Примечание После успешного восстановления БД службой DHCP значение параметра RestoreFlag автоматически изменится на 0 (значение по умолчанию).

Кроме того, для ручного восстановления БД DHCP можно, скопировав содержимое каталога %systemroot%\System32\Dhcp\Backup\Jet в папку %systemroot%\System32\Dhcp, перезапустить службу DHCP.

Ниже описаны некоторые файлы из папки %systemroot%\System32\Dhcp.

Файл	Описание
Dhcp.mdb	Файл БД DHCP
Tmp.edb	Временный файл, создаваемый службой DHCP для хранения временной информации БД в процессе работы службы
J50.log and J50*.log	Файлы журнала, хранящие записи обо всех транзакциях в БД DHCP; служба DHCP использует их для восстановления данных

Внимание! Не изменяйте и не удаляйте эти файлы.

Резюме

Служба DHCP собирает и выделяет конфигурационную информацию TCP/IP, автоматически присваивая DHCP-клиентам IP-адреса. При каждом запуске клиент DHCP запрашивает у сервера DHCP сведения об IP-адресе: собственно IP-адрес, маску подсети и необязательные параметры (например, шлюз по умолчанию). Сервер DHCP выделяет IP-адрес клиенту DHCP в 4 этапа: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST и DHCPACK. Для внедрения DHCP надо установить и настроить службу DHCP минимум на одном компьютере с Windows 2000 Server, состоящем в сети TCP/IP. Вам также следует определить и активизировать область DHCP (диапазон IP-адресов, выделяемых клиентам). Кроме того, надо авторизовать домен в Active Directory. Определив область, можно настроить параметры клиентов DHCP. Для некоторых клиентов можно зарезервировать IP-адреса, чтобы сервер DHCP всегда выделял им один и тот же IP-адрес. Чтобы задать периодичность резервного копирования БД DHCP, отредактируйте реестр Windows 2000. Кроме того, БД DHCP можно восстановить вручную, отредактировав реестр.

Занятие 4. Служба WINS

Мы обсудим назначение и работу службы WINS, а также процесс регистрации имен. Мы рассмотрим также конфигурирование клиента и сервера WINS, поддержку клиентов, не использующих WINS, и настройку WINS на клиенте DHCP с помощью оснастки DHCP.

Изучив материал этого занятия, Вы сможете:

- ✓ описать назначение и работу службы WINS, включая регистрацию, продление аренды и освобождение имен;
- ✓ внедрить WINS в среде Windows 2000.

Продолжительность занятия - около 35 минут.

Введение в WINS

В смешанной сетевой среде клиенты низкого уровня, например Windows 98/NT 4.0-компьютеры, устанавливают связь, используя имена NetBIOS. Поэтому сети Windows 2000, если в ней есть клиенты низкого уровня, нужны средства для преобразования имен NetBIOS в IP-адреса. WINS — это усовершенствованная версия сервера имен NetBIOS, регистрирующая NetBIOS-имена компьютеров и преобразующая их в IP-адреса. WINS также поддерживает динамическую БД, обеспечивающую привязку имен компьютеров к IP-адресам.

Примечание О WINS см. также документ \chapt09\articles\WINS2000.doc на прилагаемом компакт-диске.

Процесс преобразования имен службой WINS

Процесс преобразования имен службой WINS позволяет клиентам WINS регистрировать свои имена и IP-адреса на сервере WINS. Клиенты WINS выполняют запросы к серверам WINS для поиска и взаимодействия с ресурсами сети.

Процесс преобразования имен службой WINS включает следующие этапы.

1. При каждом запуске клиент WINS регистрирует привязку «NetBIOS-имя/IP-адрес» на соответствующем сервере WINS.

   Примечание При изменении сведений об IP-адресе клиент WINS автоматически обновляет БД WINS. Такое обновление, например, производится, когда служба DHCP динамически присваивает новый адрес компьютеру, перемещенному из одной подсети в другую.

2. При формировании команды NetBIOS для установки связи с другим ресурсом клиент WINS отсылает запрос на определение имени прямо серверу WINS без широковещательной рассылки такого запроса в ЛВС.
3. Сервер WINS находит в БД привязку «NetBIOS-имя/IP-адрес», соответствующую требуемому ресурсу, и возвращает клиенту WINS IP-адрес этого ресурса.

Регистрация имени

Для каждого клиента WINS определен IP-адрес первичного и вторичного (необязательно) сервера WINS. При запуске клиент регистрирует свои NetBIOS-имя и IP-адрес, отсылая определенному для него серверу WINS запрос на регистрацию.

Если сервер WINS доступен и запрашиваемое имя не зарегистрировано другим клиентом WINS, сервер отсылает клиенту сообщение об успешной регистрации. Сообщение включает срок, на который имя зарегистрировано для клиента (time to live, TTL). Кроме того, сервер WINS заносит в БД привязку «NetBIOS-имя/IP-адрес», соответствующую данному клиенту.

Если имя уже зарегистрировано в БД сервера WINS

Сервер отсылает текущему владельцу имени запрос на определение имени. Запрос отсылается трижды с интервалом в 500 миллисекунд. Если же зарегистрированный компьютер подключен к нескольким физическим линиям данных, т. е. на нем установлено несколько сетевых адаптеров, привязанных к TCP/IP и обладающих уникальными IP-адресами, сервер WINS будет проверять все IP-адреса компьютера, пока не получит отклик или не переберет все адреса.

Если текущий владелец успешно ответит серверу WINS, тот перешлет клиенту, пытавшемуся зарегистрировать имя, отказ в регистрации. Но если текущий владелец имени не отвечает, сервер WINS перешлет клиенту, пытавшемуся зарегистрировать имя, подтверждение регистрации.

Если сервер WINS недоступен

Клиент WINS трижды пытается найти первичный WINS-сервер. В случае ошибки он посылает запрос на регистрацию имени вторичному серверу WINS (если таковой определен). Если оба сервера недоступны, клиент генерирует 3 рассылки B-узла по локальной сети. Если в локальной сети существует запрашиваемое NetBIOS-имя, оно будет разрешено в IP-адрес.

Продление аренды имени

Сервер WINS регистрирует все NetBIOS-имена на временной основе, чтобы и другие компьютеры могли использовать эти имена после освобождения их исходными владельцами. Поскольку сервер WINS регистрирует имя лишь на время, клиенту приходится продлять срок аренды имени, чтобы тот не истек,

Для использования старого NetBIOS-имени клиент должен продлять срок аренды до истечения последнего. Если клиент не обновил период аренды, сервер WINS делает NetBIOS-имя доступным другим клиентам.

Первую попытку продлить срок аренды имени клиент WINS делает по истечении 1/8 интервала TTL. Если клиент не получит ответа, продляющего срок аренды, он будет отсылать запросы на продление каждые 2 минуты до истечения половины периода TTL.

По прошествии половины интервала TTL клиент WINS пытается продлить срок аренды, запросив вторичный сервер WINS (если он определен). При переключении на вторичный сервер считается, что клиент WINS пытается продлить срок аренды впервые. Это значит, что клиент будет отсылать запросы через 1/8 интервала TTL, пока не получит ответ, продляющий срок аренды, или пока не истечет половина интервала TTL (4 запроса). Затем клиент WINS переключится на первичный сервер WINS.

Получив запрос на продление аренды, сервер WINS отсылает клиенту ответ с новым интервалом TTL. Если первая попытка продления аренды имени была успешной, вторая будет сделана лишь по истечении половины интервала TTL.

Освобождение имени

Если NetBIOS-имя больше не требуется, клиент WINS сообщает серверу WINS об освобождении имени. При корректном выключении клиент WINS отсылает серверу запрос, включающий IP-адрес клиента и его NetBIOS-имя, на освобождение каждого зарегистрированного имени.

При получении запроса на освобождение имени сервер WINS проверяет наличие указанного имени в своей БД. Если в БД будет обнаружена ошибка или к зарегистрированному имени окажется привязанным другой IP-адрес, сервер WINS откажет клиенту в освобождении имени. В противном случае сервер подтверждает освобождение имени и отмечает в БД это имя как освобожденное. Ответ об освобождении имени включает NetBIOS-имя и значение TTL, равное 0.

Запрос на определение имени

После регистрации своего NetBIOS-имени и IP-адреса на сервере WINS клиент может устанавливать связь с другими узлами, получая с сервера WINS IP-адреса других компьютеров, использующих NetBIOS.

По умолчанию клиент WINS пытается разрешить NetBIOS-имя узла в IP-адрес:

1. клиент проверяет свой кэш NetBIOS-имен на наличие привязки «NetBIOS-имя/IP-адрес», соответствующей конечному компьютеру;
2. если клиент не может разрешить имя, используя кэш, он посылает запрос на определение имени своему первичному серверу WINS;
3. при недоступности первичного сервера WINS клиент отошлет запрос еще дважды и переключится на вторичный сервер WINS;
4. если любой из серверов WINS (первичный или вторичный), разрешит имя, он пошлет клиенту ответ с IP-адресом, соответствующим запрошенному NetBIOS-имени;
5. если ни один из серверов WINS не сможет разрешить имя, клиент получит сообщение о том, что запрошенное имя не существует, и начнет широковещательную рассылку в сети.

Примечание Все WINS-коммуникации осуществляются с применением направленных дейтаграмм UDP через порт 137 (служба имен NetBIOS).

Внедрение WINS

Для внедрения WINS надо настроить службу WINS на компьютере с Windows 2000 Server и некоторые параметры на клиентах WINS.

Настройка сервера WINS

Сервер WINS устанавливается на компьютере с Windows 2000 Server; не требуется, чтобы он был контроллером домена. Кроме того, на компьютере должна быть настроена служба WINS, ему надо присвоить статичный IP-адрес, маску подсети и шлюз по умолчанию.

Сервер WINS также может включать:

- постоянную привязку адресов для всех клиентов, не использующих WINS, — это позволит устанавливать связь с клиентами WINS в удаленных сетях;
- поддержку WINS, обеспечиваемую службой DHCP.

Настройка клиента WINS

Клиент WINS должен работать под управлением следующих ОС:

- **Windows** 2000;
- Windows NT Server 3.5 или последующих версий;
- Windows NT Workstation 3,5 или последующих версий;
- Windows98;
- Windows 95;
- Windows for Workgroups 3.11, использующей Microsoft TCP/IP-32;
- Microsoft Network Client 3.0 for Microsoft MS-DOS с драйвером реального режима TCP/IP;
- LAN Manager 2.2c for MS-DOS (LAN Manager 2.2c for OS/2 не поддерживается).

Для клиента следует также определить IP-адрес первичного и, по желанию, вторичного сервера WINS.

Установка WINS

Служба WINS устанавливается независимо от Windows 2000 Server. Для этого предназначена программа Add/Remove Programs (Установка и удаление программ).

Установив службу WINS на компьютер с Windows 2000 Server, надо изменить параметры TCP/IP так, чтобы компьютер обращался сам к себе. Для этого служит вкладка WINS диалогового окна Advanced TCP/IP Settings (Дополнительные параметры TCP/IP).

Оснастка WINS

Содержит подробную информацию о серверах WINS, имеющихся в сети, позволяет управлять и настраивать сервер WINS, просматривать содержимое БД WINS и осуществлять поиск конкретных записей (рис. 9-8).

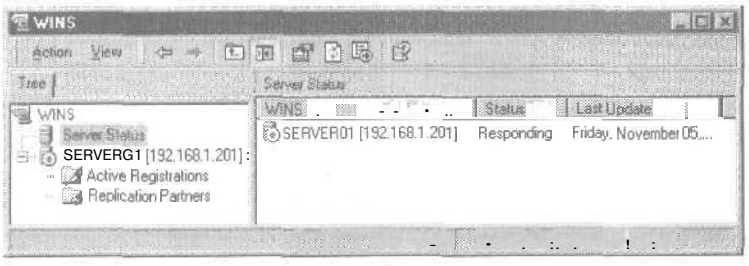


Рис. 9-8. Оснастка WINS

Оснастка DHCP запускается из консоли управления (MMC) или из узла Services And Applications дерева консоли Computer Management. Чтобы ее использовать, надо сначала установить службу WINS.

Поддержка клиентов, не использующих WINS

Для поддержки в среде WINS клиентов, не использующих эту службу, можно организовать постоянную привязку адресов и настроить агент — представитель WINS.

Постоянная привязка адресов

Для каждого из клиентов, не использующих WINS, можно организовать постоянную привязку «NetBIOS-имя/IP-адрес». Это гарантирует, что клиенты WINS смогут определять NetBIOS-имена клиентов, не использующих WINS.

Примечание Для каждого из клиентов DHCP, требующих постоянной привязки, следует зарезервировать IP-адрес.

Чтобы создать статичную привязку адреса для клиента, не использующего WINS, щелкните узел Active Registrations (Активные регистрации), а затем в меню Action (Действие) — команду New Static Mapping (Создать статическое сопоставление). При создании статичной привязки можно определить область NetBIOS. Область представляет собой необязательное расширение имени компьютера, позволяющее группировать компьютеры сети. Существует 5 типов статичной привязки адреса.

Тип	Описание
Unique (Уникальный)	Уникальное имя, привязанное к одному IP-адресу.
Group (Группа)	Имя, привязанное к группе. Добавляя в группу запись через оснастку WINS, укажите имя компьютера и IP-адрес. IP-адреса членов групп не хранятся в БД WINS, и поэтому число членом группы не ограничено.
Domain Name (Имя домена)	Привязка «NetBIOS-имя/IP-адрес», 16-й байт которой равен 0x1C. В привязке этого типа может храниться до 25 адресов членов домена. Для 26 и следующих записей WINS перезаписывает адреса реплик или, если таковых нет, перезаписывает наиболее старые записи.
Internet Group (Группа Интернета)	Определяемые пользователем группы, создаваемые для объединения ресурсов, например принтеров, для упрощения доступа и просмотра. В записи этого типа может храниться до 25 адресов. И все же динамический член группы не заменяет статичного члена группы, добавляемого через оснастку WINS или путем импорта файла LMHOSTS.
Multihomed (Многосетевой)	Уникальное имя, способное обладать несколькими адресами. Привязка этого типа применяется для компьютеров с несколькими сетевыми платами и может включать до 25 адресов. Для 26 и последующих адресов WINS перезаписывает адреса реплик или, если таковых нет, перезаписывает наиболее старые адреса.

Примечание После того как Вы щелкнете кнопку OK, оснастка WINS добавит статичную привязку в БД WINS. Если Вы указали неверные сведения, удалите привязку и создайте новую.

Настройка прокси-агента WINS

Прокси-агент WINS расширяет возможности сервера WINS и клиентов, не использующих WINS, в части разрешения имен, перехватывая широковещательные сообщения о регистрации имен, широковещательные запросы на разрешение имен и пересылая их серверу WINS.

- **Регистрация NetBIOS-имени.** Клиент, не использующий WINS, проводит широковещательную рассылку запроса на регистрацию имени, прокси-агент WINS пересылает этот запрос серверу WINS, чтобы убедиться, что какие-либо другие клиенты WINS не зарегистрировали искомое имя. NetBIOS-имя не регистрируется, а лишь проверяется.
- **Разрешение NetBIOS-имени.** Перехватив широковещательный запрос на разрешение имени, прокси-агент WINS проверяет кэш NetBIOS-имен и пытается разрешить требуемое имя. Если имени в кэше нет, агент пересылает запрос серверу WINS. Сервер

возвращает агенту IP-адрес, соответствующий запрашиваемому NetBIOS-имени. Агент возвращает полученную информацию клиенту, не использующему WINS.

Для настройки прокси-агента WINS отредактируйте реестр на клиенте WINS, задайте параметру EnableProxy в подразделе реестра HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\ NetBT\Parameters значение 1 и перезагрузите систему.

Настройка сервера DHCP

Если компьютер — клиент DHCP, настроить поддержку WINS можно через оснастку DHCP. Она позволяет добавить и настроить параметр области действия DHCP — 044 WINS/NBNS Servers (044 WINS/NBNS-серверы), а также указать адреса первичного и вторичного серверов (рис. 9-9).

При выделении адреса или продлении аренды адреса клиенту DHCP передается данный параметр области действия DHCP, и клиент конфигурируется для поддержки WINS.

Примечание Если для клиента указаны IP-адреса первичного и вторичного серверов WINS, они переопределят соответствующие параметры, предоставляемые сервером DHCP.

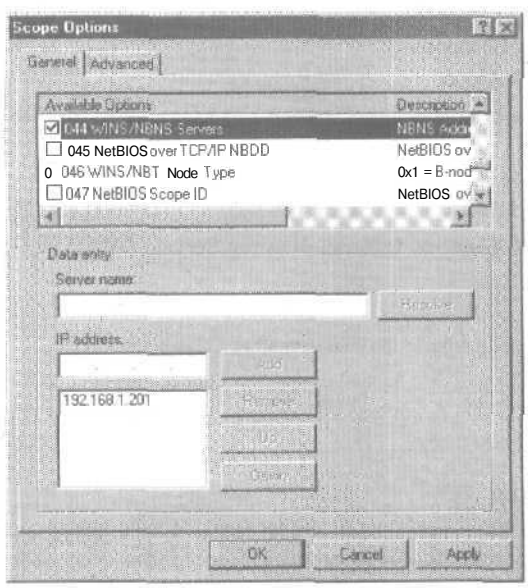


Рис. 9-9. Диалоговое окно Scope Options (Область — параметры) оснастки DHCP

Чтобы задать тип узла, настройте параметр 046 WINS/NBT Node Type (046 Тип узла WINS/NBT). Типы узлов включают в себя B-узел, P-узел, M-узел и H-узел.

Примечание Подробнее о типах узлов см. RFC I001 и RFC I002. RFC (Request for Comment) — документ, в котором описан стандарт, протокол или опубликована другая информация по работе Интернета. RFC издается после обсуждения и выступает как стандарт. Текст любого документа RFC (а также большую часть материалов для обсуждения), упомянутого в данной книге, можно найти в Интернете. Найти нужные RFC поможет Web-браузер. В данном случае выполните поиск по фразам «RFC 1001» и «RFC 1002». (Предыдущие главы включали в себя RFC, чтобы помочь Вам понять, как эти документы организованы.)

Упражнение 3: установка и настройка WINS

Вы установите WINS на Server01 и настроите параметры службы DHCP, обеспечивающие поддержку WINS. Убедитесь, что установочный компакт-диск Windows 2000 Server — в CD-ROM-приводе Server01.

Примечание Служба WINS нужна лишь для поддержки устаревшего оборудования. В Вашей небольшой учебной сети, а также в однородных сетях, включающих серверы и клиенты Windows 2000, служба WINS не требуется, так как для разрешения имен компьютеры с Windows 2000 используют DNS. Это упражнение предназначено для обучения установке и настройке WINS.

▶ Задание 1: установите WINS

Вы установите службу WINS на Server01.

1. Зарегистрируйтесь на ServerOl как Administrator с паролем **password.**
2. Раскройте меню Start\Settings (Пуск\Настройка) и щелкните Control Panel (Панель управления).
3. Дважды щелкните значок Add/Remove Programs.
4. Щелкните кнопку Add/Remove Windows Components.

   Откроется окно мастера компонентов Windows.
5. В перечне компонентов щелкните Networking Services (Сетевые службы), но не трогайте флажок напротив него.
6. Щелкните кнопку Details (Состав).

   Откроется диалоговое окно Networking Services (Сетевые службы).

   В списке компонентов пометьте флажок Windows Internet Naming Service (WINS).
7. Щелкните кнопку OK.
8. Щелкните кнопку Next (Далее).

   В соответствующие папки ОС будут скопированы файлы службы DHCP
9. Щелкните кнопку Finish (Готово).
10. Закройте окно Add/Remove Programs.
11. Закройте окно Control Panel (Панель управления).

▶ Задание 2: настройте DHCP для поддержки WINS

Вы настроите параметры WINS с помощью оснастки DHCP на ServerOl. Чтобы набраться опыта в настройке параметров сервера, Вы воспользуетесь узлом Server Options (Параметры сервера). Если Вам понадобится применить эти параметры лишь к определенной области DHCP или к конкретному DHCP-клиенту, задействуйте узел Scope Options (Параметры области).

1. На ServerOl откройте оснастку DHCP.
2. В дереве консоли щелкните папку Server Options (Параметры сервера).
3. Прочитайте сообщение на правой панели.
4. В меню Action (Действие) выберите команду Configure Options (Настроить параметры).

   Откроется диалоговое окно Server Options (Сервер — параметры).
5. Пометьте флажок 044 WINS/NBNS Servers (044 WINS/NBNS-серверы).
6. В поле Server name (Имя сервера) наберите ServerOl и щелкните кнопку Resolve (Сопоставить).

   IP-адрес компьютера ServerOl — 192.168.1.201— появится в поле IP Address (IP-адрес).

7. Щелкните кнопку Add (Добавить).
8. Прокрутите список до появления параметра 046 WINS/NBT Node Type (046 Тип узла WINS/NBT) и щелкните его флажок.
9. В текстовом поле наберите 8, чтобы в поле значилось 0x8. Значение 0x8 соответствует типу узла h. Тип узла определяет порядок разрешения имен службой WINS на клиенте.
10. Щелкните кнопку OK.

    На правой панели появятся два параметра сервера.
11. Закройте оснастку DHCP.

► **Задание 3: проверьте параметры WINS (необязательный этап)**

Вы продлите аренду и освободите зарезервированный IP-адрес на Server02, затем запустите оснастку WINS на Server01 и убедитесь, что Server02 зарегистрирован в БД WINS.

Примечание Если Вы только включили Server02, перейдите к п. 4; пп. 1-3 нужны лишь для продления аренды IP-адреса.

1. На Server02 откройте сеанс MS-DOS.
2. В командной строке введите **ipconfig** /release и нажмите Enter.

   Появится сообщение, что IP-адрес, занимаемый адаптером Local Area Connection (Подключение по локальной сети), освобожден.
3. Введите **ipconfig /renew** и нажмите клавишу Enter.
4. Введите ipconfig /all | more и нажмите клавишу Enter.
5. Нажимая при необходимости Enter, просмотрите настройки локального адаптера.

   Значение параметра Node Type (тип узла) равно Hybrid (эквивалент h-node), а адрес первичного сервера WINS указан как 192.168.1.201 (IP-адрес ServerOl).
6. На Server02 закройте окно сеанса MS-DOS.
7. На ServerOl раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и выберите WINS.

   Откроется окно оснастки WINS.
8. Разверните его.
9. Раскройте узел SERVER01 [192.168.1.201] и щелкните папку Active Registrations (Активные регистрации).
10. Прочитайте сообщение, появившееся в панели деталей.
11. В меню Action (Действие) выберите команду Find By Name (Найти по имени).
12. В открывшемся окне в поле Find Names Beginning With (Искать имена, начинающиеся с) введите Ser и щелкните кнопку Find Now (Найти).

    Server02 будет представлен тремя записями — службами, осуществляющими широковещательную рассылку имени Server02 в сети. Первая — 00h — NetBIOS-имя компьютера, 03h применяется для приема и передачи широковещательных сообщений, 20h — для доступа к Server02 другим компьютерам сети.
13. Закройте оснастку WINS.

Резюме

Регистрация имени — важнейшая часть процесса разрешения имен. Для каждого клиента WINS определен IP-адрес первичною и вторичного сервера WINS. При запуске клиент регистрирует свои NetBIOS-имя и IP-адрес, отсылая определенному для него серверу WINS запрос на регистрацию. Сервер WINS регистрирует NetBIOS-имена на временной основе, и поэтому клиенту WINS надо продлять аренду имени, иначе ее срок истечет. Получив запрос на продление аренды, сервер WINS отсылает клиенту сообщение о продлении, включающее новое значение TTL. Кроме того, если клиенту WINS больше не требуется NetBIOS-имя, он сообщает серверу WINS об освобождении имени. Получив запрос на освобождение имени, сервер WINS проверяет наличие указанного имени в своей БД. Обнаружив соответствующую привязку «NetBIOS-имя/IP-адрес», он подтвердит клиенту освобождение имени и пометит в БД имя как освобожденное. Для внедрения WINS надо установить и настроить службу WINS на компьютере с Windows 2000 Server. Кроме того, надо настроить некоторые параметры на клиентах WINS. Оснастка WINS предоставляет подробную информацию о серверах WINS, имеющихся в сети. Оснастка также позволяет просматривать содержимое БД WINS и осуществлять поиск конкретных записей.

Занятие 5. Служба DNS

DNS — это распределенная база данных в сетях TCP/IP для преобразования имен компьютеров (имен узлов) в IP-адреса. На этом занятии Вы узнаете о DNS и разрешении имен, а также об установке и настройке службы DNS.

Изучив материал этого занятия, Вы сможете:

- ✓ объяснить назначение DNS и ее компонентов, а также описать процесс разрешения имен;
- ✓ установить и настроить службу DNS, включая Dynamic DNS и службу DHCP для DNS;
- ✓ настроить клиент DNS;
- V разрешить проблемы со службой DNS.

Продолжительность занятия — около 90 минут.

Введение в DNS

Понятие DNS обычно ассоциируется с Интернетом. Однако DNS активно применяется в частных сетях для разрешения имен узлов и определения местоположения компьютеров в ЛВС и Интернете. Разрешение имен DNS отличается от разрешения имен WINS. WINS преобразует NetBIOS-имена в IP-адреса, а DNS — имена узлов в IP-адреса. IP-имена узлов, разрешенные с помощью DNS или других средств, обеспечивают следующие преимущества:

- IP-имена хостов более дружественны, т. е. запоминать IP-имена легче, чем IP-адреса;
- IP-имена узлов более стабильны, чем IP-адреса. IP-адрес сервера может измениться, а имя сервера останется прежним;
- IP-имена хостов позволяют пользователям подключаться к локальным серверам по тем же правилам именования, что и в Интернете.

Примечание О DNS см. RFC 1034 и RFC 1035. В Web-обозревателе выполните поиск по фразам «RFC 1034» и «RFC 1035». Кроме того, о DNS и о реализации DNS см. документ \chapt09\articles\w2kDNS.doc на прилагаемом компакт-диске.

Пространство имен домена

Это схема именования, обеспечивающая иерархичную структуру БД DNS. Каждый узел представляет раздел БД DNS и называется доменом.

БД DNS индексируется по имени, т. е. у каждого домена должно быть имя. При добавлении доменов в иерархичную структуру имя родительского домена добавляется к именам его дочерних доменов (поддоменов). Следовательно, имя домена определяет его положение в иерархии. Например, имя sales.microsoft.com указывает, что домен sales состоит в домене microsoft, а домен microsoft является поддоменом домена com (рис. 9-10).

Структура пространства имен домена включает корневой домен, домены верхнего и второго уровней и имена узлов.

Примечание Понятие «домен» в контексте DNS имеет несколько иное значение, чем в контексте службы каталогов Microsoft Windows 2000. В Windows 2000 домен — это объединение компьютеров и устройств, администрируемых как одно целое. В DNS домен — это узел, представляющий раздел БД DNS.

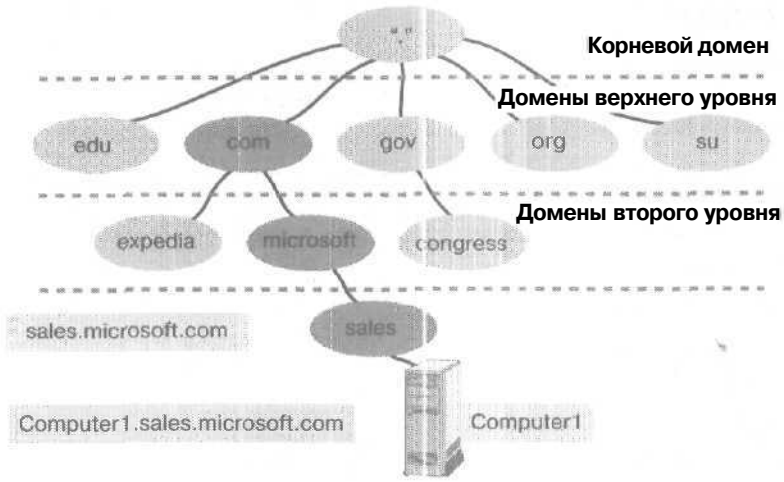


Рис. 9-10. Иерархическая структура пространства имен домена

Корневой домен

Корневой домен находится на вершине иерархии и обозначается точкой (.). Корневой домен Интернета обслуживается несколькими организациями, в том числе и Network Solutions, Inc.

Домены верхнего уровня

Домены верхнего уровня являются 2- или 3-символьными кодами имен. Домены верхнего уровня распределяются по типу или географическому расположению организации. Ниже дается несколько примеров имен доменов верхнего уровня.

Домен верхнего уровня	Описание
gov	Правительственные организации
com	Коммерческие организации
edu	Образовательные учреждения
org	Некоммерческие организации
га	Код России

Домен верхнего уровня может включать домены второго уровня и имена хостов.

Домены второго уровня

Такие организации, как Network Solutions, Inc., выделяют и регистрируют для частных лиц и организаций домены Интернета второго уровня. Домен второго уровня может включать как узлы, так и поддомены. Допустим, microsoft.com включает компьютеры, например, ftp.microsoft.com, и поддомены, например, dev.microsoft.com. Поддомен dev.microsoft.com. может включать узлы, например, printerserver1.dev.microsoft.com.

Имена узлов

Ссылаются на конкретные компьютеры в Интернете или частной сети. Например, имя Computerl является именем хоста (рис. 9-10). Имя хоста — это левая часть *полного доменного имени* (fully qualified domain name, FQDN), описывающего точное положение узла в иерархии домена. На рис. 9-10 Computer1.sales.microsoft.com. (включая последнюю точку,

представляющую корневой домен) — полное доменное имя. DNS использует полное доменное имя хоста при разрешении имени в IP-адрес.

Примечание Имя узла не обязательно должно совпадать с именем компьютера. По умолчанию программа установки протокола TCP/IP в качестве имени узла использует имя компьютера, заменяя недопустимые символы, например знаки подчеркивания (_), дефисами (-). Подробнее о принятых соглашениях по именованию доменов см. RFC 1035.

Правила именования доменов

При создании пространства имен домена помните следующее.

- Ограничивайте число уровней домена. Обычно записи узлов должны стоять на 3 или 4, но не более, чем на 5 уровней ниже по иерархии DNS. При увеличении числа уровней увеличивается объем задач администрирования.
- Используйте уникальные имена. Чтобы в пространстве имен DNS были лишь уникальные имена, в домене не должно быть поддоменов с идентичными именами.
- Используйте простые уникальные имена. Простые и точные имена доменов легче запоминаются и делают возможным интуитивный поиск Web-узлов и других компьютеров в Интернете и интрасети.
- Избегайте длинных имен. Доменное имя может включать до 63 символов с учетом точек. Общая длина полного доменного имени не может превышать 255 символов. В именах не учитывается регистр.
- Используйте стандартные символы DNS и Unicode:
  - Windows 2000 поддерживает стандартные символы DNS, определенные в RFC 1035: A–Z, a-z, 0-9 и дефис (-);
  - служба **DNS** поддерживает набор символов Unicode, включающий дополнительные символы, не заложенные в набор символов ASCII, но нужные таким языкам, как французский, немецкий и испанский.

Примечание Используйте символы Unicode, только если они поддерживаются всеми серверами Вашей сети. Подробнее о наборе символов Unicode см. RFC 2044, выполнив с помощью обозревателя Web поиск по фразе «RFC 2044».

Зоны

Зона — это отдельная часть пространства имен домена. Зоны позволяют делить пространство имен домена на управляемые секции.

Для распространения административных задач по группам пространство имен домена делится на несколько зон. Например, на рис. 9-11 пространство имен домена microsoft.com разделено на две зоны. Благодаря этому один администратор может управлять доменами microsoft и sales, а другой — доменом development.

Зона должна охватывать непрерывное пространство имен домена. Например, можно создать зону, охватывающую sales.microsoft.com и родительский домен microsoft.com, поскольку эти зоны связаны (рис. 9-11). Однако создать зону, содержащую только домены sales.microsoft.com и development.microsoft.com, нельзя, поскольку эти домены не связаны.

Используемые в зоне привязки «IP-адрес/имя» хранятся в файле БД зоны. Каждая зона прикреплена к определенному домену — корневому домену зоны. Файл БД зоны может содержать сведения не обо всех поддоменах корневого домена зоны.

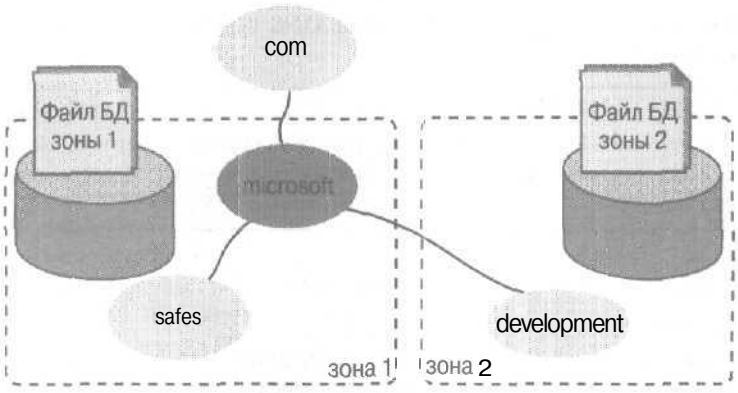


Рис. 9-11. Пространство имен домена, разделенное на две **зоны**

На рис. 9-11 microsoft — корневой домен зоны 1, файл БД которой содержит привязки «IP-адрес/имя» для доменов microsoft и sales. Корневым доменом зоны 2 является домен development, и файл БД этой зоны содержит привязки «IP-адрес/имя» лишь для домена development. Файл БД зоны 1 не содержит привязок «IP-адрес/имя» для домена development, хотя тот и является поддоменом домена microsoft.

Серверы имен DNS

Хранят файлы БД зон. На сервере могут размещаться БД нескольких зон. Сервер имен обладает полномочиями в пространстве имен, охватываемом зоной.

В зоне должен иметься хотя бы один сервер имен, но их может быть и несколько. Один из них содержит мастер-файл БД этой зоны, или первичный файл БД зоны. Изменения в конфигурации зоны, например добавление доменов или хостов, обрабатываются на сервере, содержащем первичный файл БД зоны. Все остальные серверы имен, связанные с данной зоной, являются резервными и содержат вторичные файлы БД.

Наличие множества серверов имен дает Вам некоторые преимущества.

- **Передача зоны** — дополнительные серверы имен получают от сервера, содержащего первичный файл БД зоны, копию этого файла. Это называется передачей зоны. Резервные серверы периодически обращаются к серверу, содержащему первичный файл БД, за обновленными сведениями о конфигурации зоны.
- **Избыточность** — при сбое сервера, содержащего первичный файл БД зоны, в работу включаются резервные серверы.
- **Повышение скорости доступа удаленных клиентов** — при наличии удаленных клиентов дополнительные серверы имен позволят снизить трафик запросов в низкоскоростных каналах связи с ГВС.
- **Снижение нагрузки** — дополнительные серверы имен уменьшают нагрузку на сервер, содержащий первичный файл БД зоны, Кроме того, благодаря БД Active Directory Windows 2000 поддерживает хранилище зоны, интегрированное с каталогом. Зоны, хранимые подобным образом, содержатся в дереве Active Directory в объекте-контейнере Domain. Каждая зона, интегрированная с каталогом, хранится в объекте-контейнере зоны DNS, которому присваивается имя зоны.

Обзор процесса разрешения имен

Разрешение имен — это процесс преобразования имен в IP-адреса, похожий на поиск имени в телефонной книге, где имя связано с номером телефона. Например, подключаясь к Web-узлу компании Microsoft, Вы используете имя www.microsoft.com. DNS разрешает это имя в соответствующий IP-адрес. Привязки «IP-адрес/имя» хранятся в распределенной БД DNS.

Серверы имен DNS разрешают прямые и обратные запросы на поиск имени. Прямой запрос разрешает имя в IP-адрес. Обратный запрос разрешает IP-адрес в имя. Сервер имен может разрешать запросы лишь для той зоны, в которой он обладает полномочиями. Если сервер не может разрешить запрос, он передает его другому серверу имен, который сможет это сделать. Для снижения DNS-трафика в сети сервер имен кэширует результаты запроса.

Прямой запрос на поиск имени

Для разрешения имен служба DNS использует модель клиент — сервер. Клиент передает прямой запрос на поиск имени локальному серверу имен. Этот сервер разрешает запрос сам или передает его другому серверу имен.

На рис. 9-12 показан процесс запроса клиентом IP-адреса, соответствующего имени www.microsoft.com; цифры соответствуют следующим этапам.

1. Клиент передает прямой запрос на поиск имени www.microsoft.com локальному серверу имен.
2. Локальный сервер имен проверяет файл БД своей зоны на наличие соответствующей связки «IP-адрес/имя». Не имея полномочий в домене microsoft.com, локальный сервер имен передает запрос одному из корневых серверов DNS, запрашивая разрешение имени узла. Корневой сервер возвращает ссылку на серверы имен домена com.
3. Локальный сервер имен посылает запрос серверу имен домена com, и тот возвращает ссылку на серверы имен домена microsoft.

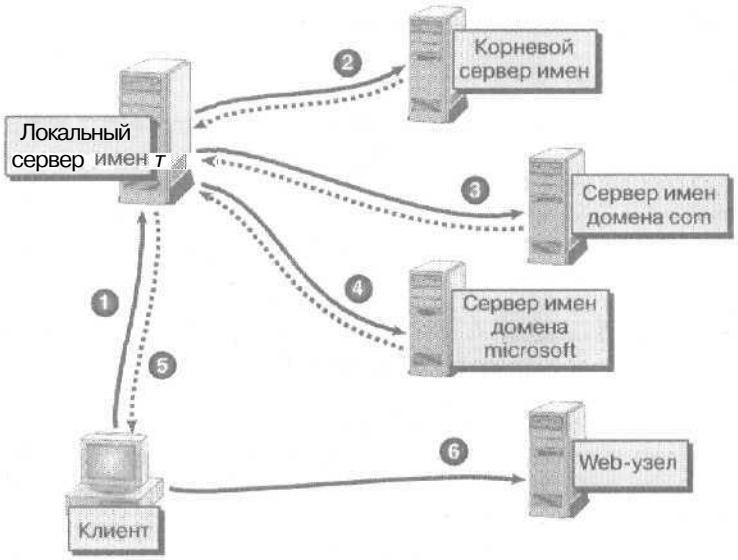


Рис. 9-12. Разрешение прямого запроса на поиск имени

4. Локальный сервер имен посылает запрос на сервер имен домена microsoft, и тот принимает запрос. Обладая правами в этой части пространства имен домена, сервер имен домена microsoft возвращает локальному серверу имен IP-адрес, соответствующий имени www.microsoft.com.
5. Локальный сервер имен посылает IP-адрес клиенту.
6. Разрешение имени завершено, и теперь клиент может обратиться к узлу www.microsoft.com, используя его IP-адрес.

Кэширование на сервере имен

При обработке запроса сервером имен для получения ответа, возможно, придется отправить несколько запросов. Выполняя запросы, сервер выясняет расположение других серверов имен, обладающих правами в соответствующих частях пространства имен. Для снижения трафика сервер имен кэширует результаты этих запросов.

При получении результата;

1. сервер имен кэширует результат запроса на некоторый срок (TTL); этот период (по умолчанию — 60 минут) определяется зоной, предоставившей результаты запроса; TTL задается через оснастку DNS;
2. после того как сервер поместил результаты запроса в кэш, начинается обратный отсчет времени;
3. по истечении TTL сервер имен удаляет результаты запроса из кэша.

Кэширование результатов запроса позволяет серверу быстрее разрешать другие запросы, обращенные к той же части пространства имен домена.

Примечание Небольшой TTL позволит гарантировать, что данные о пространстве имен домена не устарели. Хотя такие значения TTL и повышают нагрузку на сервер имен, а длительные периоды сокращают сроки разрешения имен, клиент будет получать устаревшую информацию, пока не истечет TTL и не будет выполнен новый запрос к этой части пространства имен домена.

Обратный запрос на поиск имени

Разрешает имя в IP-адрес; служебные программы, например nslookup, используют обратные запросы для вывода имен узлов. Кроме того, некоторые приложения реализуют защиту, основанную на подключении с использованием имен, а не IP-адресов.

Поскольку распределенная БД DNS индексируется по имени, а не по IP-адресу, при обработке обратного запроса должен производиться полный перебор всех доменных имен. Для решения этой проблемы создан специальный домен второго уровня in-addr.arpa.

Этот домен придерживается той же иерархичной системы именования, но основывается не на доменных именах, а на IP-адресах:

- поддоменам присваиваются имена, соответствующие IP-адресам (4 октета, разделенные точками);
- порядок октетов IP-адреса меняется на противоположный;
- организации администрируют поддомены домена in-addr.arpa, основываясь на назначенных им IP-адресах и маске подсети.

Например, организация, которой выделен диапазон IP-адресов от 169.254.16.0 до 169.254.16.255 с маской подсети 255.255.255.0, обладает полномочиями в отношении домена 16.254.169.in-addr.arpa.

Установка службы DNS

Для внедрения DNS надо настроить сервер и установить службу DNS. Сервер DNS должен обладать статичным IP-адресом. Параметры TCP/IP следует сконфигурировать так, чтобы настройки DNS указывали обратно на сервер. Установить службу DNS можно в любое время после или в процессе установки Windows 2000 Server.

Процесс установки DNS;

- устанавливает оснастку DNS и добавляет в меню Administrative Tools (Администрирование) соответствующий ярлык; оснастка DNS служит для управления локальными и удаленными серверами имен DNS;
- добавляет в реестр раздел, используемый службой DNS, — HKEY_LOCAL_ MACHTNE\System\CurrentControlSet\Services\DNS;
- создает папку %systemroot%\System32\DNS, содержащую файлы БД DNS.

Обычно редактировать файлы БД DNS не надо, хотя их можно использовать при устранении неполадок DNS. Служба DNS представляет Вам набор файлов-примеров; при установке службы DNS они копируются в папку %systemroot%\System32\DNS\Samples.

Примечание В папке %systemroot%\System32\DNS\Samples есть файл BOOT, не определенный в RFC. Однако он является частью реализации DNS, использующей BIND (Berkeley Internet Name Daemon). Если у Вас ранее использовался сервер DNS, работавший под управлением BIND, для перемещения существующей конфигурации скопируйте файл BOOT

Конфигурирование службы DNS

После установки службы DNS можно перейти к ее настройке и обслуживанию.

Оснастка DNS

Оснастка DNS (рис. 9-13) служит для настройки зон прямого и обратного поиска, добавления в файл БД зоны записей о ресурсах, конфигурирования службы DNS для использования *динамической системы доменных имен* (Dynamic DNS, DDNS), позволяющей другим серверам и службам автоматически обновлять файлы Вашей зоны.

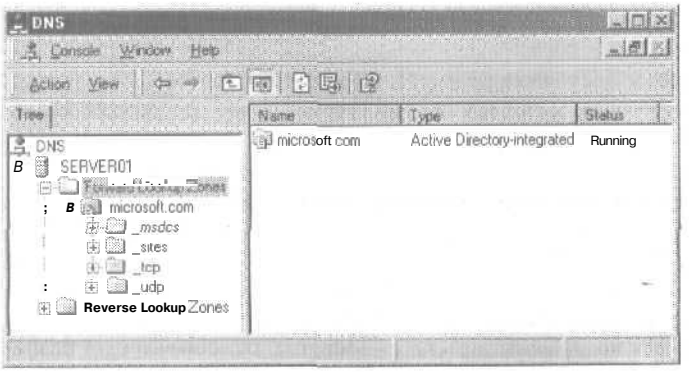


Рис. 9-13. Оснастка DNS

Оснастку DHCP можно запустить из консоли управления (MMC) или из узла Services And Applications (Службы и приложения) дерева оснастки Computer Management (Управление компьютером), Для установки оснастки DNS можно выполнить файл Adminpak.msi

или установить службу DNS. При отсутствии службы DNS оснастка используется для управления удаленными серверами, на которых установлена служба DNS.

Создание зон прямого просмотра

Зона прямого просмотра позволяет генерировать прямые запросы поиска имени. Для работы службы DNS на сервере имен надо сконфигурировать не менее одной зоны прямого просмотра.

Чтобы создать новую зону прямого просмотра, щелкните папку Forward Lookup Zone (Зона прямого просмотра) и в меню Action (Действие) выберите команду New Zone (Создать новую зону). Создать зону Вам поможет мастер.

Тип зоны

Вы можете создать зону одного из трех типов.

- **Active Directory-integrated (Интегрированная в Active Directory).** Главная копия новой зоны, использует для хранения и репликации файлов зоны службу Active Directory. Зоны такого типа обеспечивают безопасное обновление и интегрированное хранение. Стандартные зонные передачи не осуществляются — файл БД зоны реплицируются одновременно с хранилищем Active Directory.
- **Standard primary (Основная).** Главная копия новой зоны, хранится как обычный текстовый файл. Администрирование и поддержка основной зоны осуществляется на том компьютере, где была создана. Зоны такого типа упрощают обмен DNS-данными с другими серверами DNS, хранящими данные в виде текста.
- **Standard secondary (Дополнительная).** Реплика сушествующей зоны, хранится в обычных текстовых файлах и доступна только для чтения. Для создания дополнительной зоны надо сначала создать основную. При создании надо указать основной DNS-сервер, который передает информацию о зоне на сервер имен, содержащий дополнительную зону. Дополнительные зоны создаются для обеспечения избыточности и уменьшения нагрузки на сервер имен, содержащий основной файл БД зоны.

Имя зоны

Обычно зоне присваивается имя наивысшего домена в иерархии, охватываемой зоной, т. е. имя корневого домена зоны. Например, зоне, включающей домены microsoft.com и sales.microsoft.com, будет присвоено имя microsoft.com.

Файл зоны

Это имя файла БД, по умолчанию состоящее из имени зоны с расширением .dns. Например, если имя зоны — microsoft.com, файл БД по умолчанию будет называться microsoft.com.dns.

При передаче зоны с другого сервера можно импортировать существующий файл зоны. Перед созданием новой зоны этот файл надо поместить в папку конечного компьютера %systemroot%\System32\DNS. Зона передается одним из двух способов: полным (запрос AXFR) и добавочным (запрос IXFR). AXFR — стандартный способ передачи информации о зоне и по сути представляет собой копирование файла зоны. Помимо AXFR, Windows 2000 поддерживает и запрос IXFR, который меньше загружает линию связи, так как реплицируются только изменения в конфигурации зоны.

Создание зон обратного просмотра

Зоны обратного просмотра позволяют генерировать обратные запросы на поиск имени. Эти зоны не обязательны, однако они нужны для работы утилит устранения неполадок, например nslookup, и для фиксирования в файлах журнала служб IIS имени узла вместо его IP-адреса.

Чтобы создать новую зону обратного просмотра, щелкните папку Reverse Lookup Zone (Зона обратного просмотра) и в меню Action (Действие) — команду New Zone (Создать новую зону).

Тип зоны

Соответствуют типам зон прямого просмотра: интегрированная в Active Directory, основная и дополнительная.

Зона обратного просмотра

Укажите идентификатор Вашей сети (network ID) или имя зоны обратного просмотра. Если в идентификаторе сети указан 0, он появится в имени зоны. Например, для идентификатора сети 169 будет создана зона 169.in-addr.arpa, а для идентификатора сети 169.0 — зона 0.169.in-addr.arpa.

Файл зоны

Имя файла зоны по умолчанию определяется идентификатором сети и маской подсети. DNS обращает порядок октетов IP-адреса и добавляет суффикс in-addr.arpa. Например, имя файла зоны обратного просмотра для сети 169.254 будет 254.169.in-addr.arpa.dns.

При передаче зоны с другого сервера можно импортировать существующий файл зоны. Перед созданием новой зоны этот файл надо поместить в папку целевого компьютера %systemroot%\System32\DNS.

Добавление записей о ресурсах

Создав зоны, можно добавлять записи о ресурсах при помощи оснастки DNS. Записи о ресурсах — это записи файла БД зоны. Каждая запись идентифицирует в БД конкретный ресурс. Чтобы добавить запись о ресурсе, щелкните требуемую зону и в меню Action (Действие) — команду Other New Record (Другие новые записи). В диалоговом окне Resource Record Type (Тип записи ресурса) можно создавать записи о любых ресурсах, перечисленных в списке Select A Resource Record Type (Выбор типа записи ресурса).

Существует множество типов записей ресурса. При создании зоны DNS автоматически добавляет две: Start of Authority (SOA) и Name Server (NS). SOA определяет сервер имен, являющийся в этом домене полномочным источником данных. Первой записью файла БД зоны должна быть SOA. NS представляет собой список серверов имен, выделенных конкретному домену. Сконфигурировать записи этих двух типов можно в диалоговом окне свойств требуемой зоны прямого просмотра.

С другими типами записей ресурса, включая описание каждого типа, можно познакомиться в списке Select A Resource Record Type (Выбор типа записи ресурса) — при выборе типа внизу окна отображается его описание.

Примечание О записях ресурсов см, RFC 1034, RFC 2052 и RFC 2065. в обозревателе Web выполните поиск по фразам «RFC 1034», «RFC 2052» и «RFC 2065». Подробнее о работе DNS см. книгу Пола Альбица и Крикета Лиу *DNS and BIND.* O'Reilly and Associates, Inc. 1998 г.

Настройка Dynamic DNS

Служба DNS включает возможность динамического обновления — Dynamic DNS (DDNS). При использовании DNS после изменений в конфигурации домена, в отношении которого сервер имен обладает полномочиями, надо вручную обновить файл БД зоны на первичном сервере имен. При использовании DDNS серверы имен и клиенты сети автоматически обновляют файлы БД зоны.

Динамическое обновление

Можно определить список авторизованных серверов, которые будут выполнять динамическое обновление. Список может включать дополнительные серверы имен, контроллеры домена и другие серверы, выполняющие регистрацию клиентов в сети, например серверы WINS или DHCP.

Обновление проходит в несколько этапов.

1. Клиент при помощи запроса SOA находит для регистрируемой записи первичный сервер DNS и полномочную зону.
2. Клиент посылает найденному DNS-серверу заявление или предварительное обновление, чтобы убедиться в регистрации записи. Если запись не зарегистрирована, клиент посылает соответствующий пакет динамического обновления для регистрации записи.
3. В случае сбоя при обновлении клиент попытается зарегистрировать запись на другом первичном сервере DNS, если в зоне, обладающей полномочиями для данной записи, есть несколько главных серверов. Если все первичные серверы не смогут выполнить динамическое обновление, через 5 минут будет произведена повторная попытка, а в случае неудачи — еще одна через 10 минут. Если и на этот раз произойдет ошибка, счетчик попыток обнуляется, и через 50 минут клиент заново попытается зарегистрировать запись.

Каждый компьютер с Windows 2000 пытается зарегистрировать свои записи A и PTR. Запись A, или *запись ресурса адреса узла,* содержит привязку «IP-адрес/имя»; PTR-запись, или *запись ресурса указателя,* содержит привязку «IP-адрес/имя» для компьютера, отсылающего подтверждение регистрации, Службой, фактически генерирующей динамические обновления DNS, является клиент DHCP. Клиентская служба DHCP выполняется на каждом компьютере с Windows 2000 независимо от того, настроен ли он как клиент DHCP.

DDNS и DHCP

DDNS взаимодействует со службой DHCP для поддержки синхронизированных привязок «IP-адрес/имя», соответствующих сетевым узлам. По умолчанию служба DHCP позволяет клиентам добавлять в зону свои записи A, сама же служба DHCP добавляет в зону запись PTR. По истечении срока аренды IP-адреса служба DHCP удаляет из зоны обе эти записи.

Настроить зону для поддержки DDNS позволяет оснастка DNS. Щелкните требуемую зону и в меню Action (Действие) — команду Properties (Свойства). На вкладке General (Общие) диалогового окна свойств выберите в списке Allow Dynamic Updates (Динамическое обновление) пункт Yes (Да).

Чтобы настроить сервер для отсылки динамических обновлений, вызовите оснастку DHCP и определите для сервера DHCP соответствующие серверы DNS.

Примечание Подробности о Dynamic DNS см. в RFC 2136 и RFC 2137. С помощью обозревателя Web выполните поиск по фразам «RFC 2136» и «RFC 2137». См. также документ \chapt09\articles\w2kDNS.doc на прилагаемом компакт-диске.

Упражнение 4: настройка службы DNS

Вы удалите и повторно создадите зону прямого поиска, создадите зону обратного просмотра, настроите Dynamic DNS и протестируете Ваш сервер DNS. Вам потребуются оба компьютера — Server01 и Server02.

Примечание При выполнении упражнения 1 главы 6 была автоматически установлена DNS, так как Server01, являясь изолированным сервером, не использовал DNS для разрешения имен. Установка DNS аналогична установке DHCP и WINS: DNS является компонентом Networking Services (Сетевые службы). Можете просмотреть список Networking Services и убедиться, что служба DNS установлена.

► **Задание 1: проверьте зону прямого просмотра и создайте зону обратного просмотра**

Вы удалите созданную при установке DNS зону прямого просмотра, интегрированную с Active Directory, и создадите стандартные зоны прямого и обратного просмотра.

1. Зарегистрируйтесь на ServerOl как Administrator с паролем password.
2. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык DNS.

   Откроется окно оснастки DNS.
3. Разверните окно оснастки DNS.
4. В дереве консоли раскройте узел SERVER01, а затем — папку Forward Lookup Zones (Зоны прямого просмотра).
5. Щелкните контейнер microsoft.com.
6. В меню Action (Действие) выберите команду Delete (Удалить).
7. Появится сообщение с просьбой подтвердить операцию. Щелкните кнопку OK.

   Появится предупреждающее сообщение DNS.
8. Прочитайте его и щелкните кнопку Yes (Да).
9. В меню Action (Действие) выберите команду New Zone (Создать новую зону).

   Откроется окно мастера New Zone (Мастер создания новой зоны).
10. Щелкните кнопку Next (Далее).

    Откроется окно Zone Type (Тип зоны).
11. Убедитесь, что выбран переключатель Standard Primary (Основная), и щелкните кнопку Next (Далее).

    Откроется окно Zone Name (Имя зоны).
12. Введите **microsoft.com** и щелкните кнопку Next (Далее).
13. Откроется окно Zone File (Файл зоны).
14. Убедитесь, что выбран переключатель Create A New File With This File Name (Создать новый файл) и имя создаваемого файла — microsoft.com.dns.
15. Щелкните кнопку Next (Далее).
16. Просмотрите сводку выбранных параметров и щелкните кнопку Finish (Готово).

    Откроется окно оснастки DNS.
17. Щелкните в дереве консоли узел microsoft.com.

    Заметьте: сгенерированы записи Start ofAuthority (SOA) (Начальная запись зоны), Name Server (NS) (Сервер имен) и Host (A).

    Теперь ServerOl может разрешать имена хостов в IP-адреса, используя файл основной зоны просмотра.
18. В дереве консоли щелкните папку Reverse Lookup Zones (Зоны обратного просмотра).
19. В меню Action (Действие) выберите команду New Zone (Создать новую зону).

    Откроется окно мастера создания новой зоны.
20. Щелкните кнопку Next (Далее).
21. Убедитесь, что выбран переключатель Standard Primary (Основная), и щелкните кнопку Next (Далее).

    Откроется окно Reverse Lookup Zone (Обратный просмотр).

22. Убедитесь, что выбран переключатель Network ID (Код сети). В поле под ним введите 192.168.1.

    Поле Reverse Lookup Zone Name (Имя зоны обратного просмотра) внизу окна должно выглядеть так: 1.168.192.in-addr.arpa.
23. Щелкните кнопку Next (Далее).

    Откроется окно Zone File (Файл зоны).
24. Убедитесь, что выбран переключатель Create A New File With This File Name (Создать новый фай) и имя создаваемого файла — 1.168.192.in-addr.arpa.dns.
25. Щелкните кнопку Next (Далее).
26. Просмотрите сводку выбранных параметров и шелкните кнопку Finish (Готово).

    Теперь служба DNS на Server01 может определять имена хостов, используя в качестве исходных данных адрес и подсеть хоста.

Примечание Конфигурационная информация созданной DNS обычно добавляется в службу DHCP. Вы уже добавляли эту информацию в упражнении из предыдущего раздела данной главы.

► Задание 2: настройте динамическое обновление данных DNS

Вы настроите службу DNS для поддержки динамического обновления, используя оснастку DNS на ServerOl.

1. В дереве консоли выберите папку microsoft.com, она находится в папке Forward Lookup Zones (Зоны прямого просмотра).
2. В меню Action (Действие) выберите команду Properties (Свойства).
3. В списке Allow Dynamic Updates (Динамическое обновление) выберите пункт Yes (Да) и щелкните кнопку OK.

   Сейчас Вы настроили динамическую службу DNS для зоны прямого поиска.
4. В дереве консоли выделите контейнер 192.168.1.x Subnet.
5. В меню Action (Действие) выберите команду Properties (Свойства).
6. В списке Allow Dynamic Updates (Динамическое обновление) выберите пункт Yes (Да) и щелкните кнопку OK.

   Сейчас Вы настроили динамическую службу DNS для зоны прямого просмотра.
7. Сверните окно оснастки DNS.

► Задание 3: протестируйте работу DNS

Вы убедитесь в корректной работе службы DNS и продолжите настройку из оснастки DNS.

1. На ServerOl восстановите свернутое окно оснастки DNS.
2. В дереве консоли щелкните узел SERVEROL
3. В меню Action (Действие) выберите команду Properties (Свойства).

   Откроется диалоговое окно свойств SERVER01.
4. Перейдите на вкладку Monitoring (Наблюдение).
5. В группе Select A Test Type (Выберите тип теста) пометьте флажки A Simple Query Against This DNS Server (Простой запрос к этому DNS-серверу) и Recursive Query To Other DNS Servers (Рекурсивный запрос к другим DNS-серверам).
6. Щелкните кнопку Test Now (Тест).

   В списке Test Results (Результаты теста) против обеих записей Вы увидите PASS (тест пройден). Если Вы работаете на автономном сервере, против Recursive Query (Рекурсивный запрос) Вы увидите FAIL (ошибка).

7. Щелкните кнопку OK.

   Откроется окно оснастки DNS.

8. В дереве консоли щелкните узел Reverse Lookup Zones (Зоны обратного просмотра).
9. Щелкните папку 192.168.1.x Subnet.

   Зона обратного просмотра содержит две записи, SOA и NS (см. правую панель).

10. В меню Action (Действие) выберите команду New Pointer (Создать указатель).

    Откроется диалоговое окно New Resource Record (Запись нового ресурса).

11. В четвертом октете поля Host IP Number (IP-номер узла) введите 201,
12. В поле Host Name введите **server01.microsoft.com.** (не забудьте поставить точку после слова com).
13. Щелкните кнопку OK.

    На правой панели появится запись с типом Pointer (Указатель).

14. Закройте окно оснастки DNS.
15. На ServerOl или Server02 откройте окно командной строки.
16. В командной строке введите **nslookup** и нажмите клавишу Enter.

    На ServerOl сервер по умолчанию будет указан как localhost, а адрес — как 127.0.0.1.

    На Server02 сервер по умолчанию будет указан как server01.microsoft.com, а адрес - как 192.168.1.201.

    Оба результата указывают на server01.microsoft.com. Результат вывода nslookup на Server01 — это адрес возвратной петли сервера.

17. Наберите **Is Microsoft.com**.

    Обратите внимание, что в результате этого DNS-запроса будут выведены записи NS и A.

18. Наберите **exit** и нажмите клавишу Enter.

    Закройте окно командной строки.

Настройка клиента DNS

Установив и настроив службу DNS на компьютерах с Windows 2000 Server, можно приступить к настройке клиентов DNS. Сначала убедитесь, что на клиенте установлен пакет протоколов **TCP/IP.** Установив TCP/IP на клиентах, откройте диалоговое окно его свойств (рис. 9-4), позволяющее настроить систему для автоматического получения адреса DNS (это обеспечивает сервер DHCP) или вручную указать IP-адреса предпочтительного и дополнительного серверов DNS. Для настройки дополнительных параметров DNS щелкните кнопку Advanced (Дополнительно). Чтобы задать параметры DNS, в диалоговом окне Advanced TCP/IP Settings (Дополнительные параметры TCP/IP) (рис. 9-14) перейдите на вкладку DNS. Вам потребуется указать IP-адреса одного или несколько серверов DNS. Они необходимы для работы службы DNS. Здесь можно сконфигурировать и параметры, обеспечивающие разрешение имен узлов, для которых не было указано полное доменное имя, и настроить параметры регистрации **DDNS.**

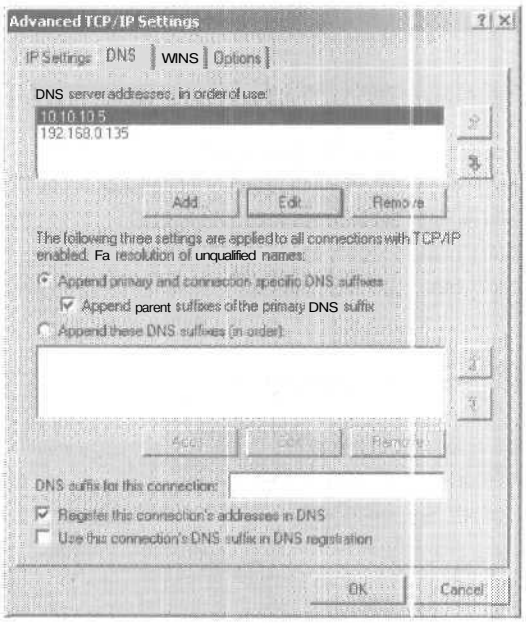


Рис. 9-14. Диалоговое окно Advanced TCP/IP Settings (Дополнительные параметры TCP/IP) с двумя адресами серверов DNS, необходимых для работы, параметрами разрешения имен и автоматической регистрации

Устранение неполадок DNS

Для устранения неполадок серверов имен применяется утилита командной строки nslookup, а также функции мониторинга и регистрации событий, доступные в оснастке DNS.

Мониторинг сервера DNS

Оснастка DNS позволяет осуществлять мониторинг службы DNS. Выберите сервер имен и в меню Action (Действие) щелкните команду Properties (Свойства). В диалоговом окне свойств перейдите на вкладку Monitoring (Наблюдение), Для проверки работы сервера имен можно выполнить запросы двух типов:

- **Simple query (Простой запрос)** — этот локальный тест использует локальный клиент DNS для создания запроса к серверу имен;
- **Recursive query (Рекурсивный** запрос) — пересылает рекурсивный запрос другому серверу имен.

Установка параметров ведения журнала

Оснастка DNS позволяет настроить дополнительные параметры ведения журнала. Открыв диалоговое окно свойств сервера имен, перейдите на вкладку Logging (Ведение журнала). Здесь доступно 11 параметров: Query (Запрос), Notify (Уведомление), Update (Обновление), Questions (Вопросы), Answers (Ответы), Send (Отправить), Receive (Получить), UDP, TCP, Full Packets (Полных пакетов) и Write Through (Запись с помощью). Информация, соответствующая выбранным параметрам, будет заноситься в файл журнала.

Утилита nslookup

Основная диагностическая утилита службы DNS — nslookup — устанавливается вместе с TCP/IP. Она позволяет просматривать записи ресурсов и пересылать запросы любому серверу имен, включая реализацию DNS для UNIX.

У nslookup два режима работы: интерактивный и неинтерактивный.

- Чтобы получить несколько блоков информации, перейдите в интерактивный режим, запустив nslookup из командной строки без дополнительных параметров; для выхода из интерактивного режима наберите **exit.**
- Если Вам хотите воспользоваться nslookup однократно, запустите ее в неинтерактивном режиме из командной строки с дополнительными параметрами:

  nslookup [*-параметр* ...] [*искомый_компьютер* - [*сервер*]]

  Ниже описаны дополнительные параметры nslookup.

Ключ	Описание
–параметр ...	Указывает один или несколько параметров nslookup. Чтобы получить список параметров, введите в интерактивном режиме знак вопроса (?).
искомый_компьютер	Если искомый компьютер представлен IP-адресом, nslookup вернет имя узла, а если именем — IP-адрес. Если компьютер представлен именем без завершающей точки, к имени добавляется имя домена DNS по умолчанию. Для поиска компьютера за пределами текущего домена DNS добавьте к имени точку.
сервер	**Указывает** сервер **имен** DNS. **Если** имя сервера опушено. **используется** сервер **имен по** умолчанию.

Резюме

DNS — это распределенная БД, используемая в сетях TCP/IP для сопоставления имен компьютеров с IP-адресами. Пространство имен домена представляет собой систему именования, обеспечивающую иерархическую структуру для БД DNS. Иерархичная структура пространства имен домена включает корневой каталог, домены верхнего и второго уровней и имена узлов. Зоны позволяют разделить пространство имен домена на управляемые секции. Зона должна охватывать непрерывное пространство имен домена. Сервер имен DNS хранит файл БД зоны и может обладать правами в отношении нескольких зон. Разрешение имен — это процесс сопоставления имен IP-адресам. Сервер имен DNS обрабатывает прямые и обратные запросы поиска имен. Прямой запрос разрешает имя в IP-адрес. Обратный запрос разрешает IP-адрес в имя. Для внедрения DNS надо установить службу DNS и настроить сервер через оснастку DNS. Оснастка DNS позволяет настраивать зоны прямого и обратного просмотра, добавлять в файл БД записи ресурсов и настраивать службу DNS для поддержки динамической DNS (DDNS), позволяющей другим серверам и службам автоматически обновлять файлы зон. Одновременно с настройкой DNS на компьютере с Windows 2000 Server надо сконфигурировать клиент Windows 2000. Для этого убедитесь, что на клиентской системе установлен TCP/IP, и в окне его свойств настройте параметры DNS. Для устранения неполадок DNS применяется утилита командной строки nslookup, а также функции мониторинга и регистрации событий, доступные в оснастке DNS.

Закрепление материала

Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Ваш компьютер получает конфигурационные сведения TCP/IP от сервера DHCP. Получив эти сведения, Вы можете подключиться к любому узлу своей подсети, а связаться или опросить какой-нибудь узел в удаленной подсети — нет. Вы проверили службу DHCP и убедились, что для Вашей области адресов указана корректная информация о маршрутизаторе. В чем вероятная: причина проблемы и как ее устранить?

2. Установив NWLink IPX/SPX и GSNW, Вы не можете связаться с одним из серверов NetWare. При подключении к этому серверу с клиента Windows 2000 Professional, на котором установлены протокол NWLink IPX/SPX и служба CSNW, проблем не возникает. Вам надо обеспечить взаимодействие Windows 2000 Server с этим сервером NetWare, поскольку последний содержит ресурсы, которые Вам надо предоставить пользователям с сетевым клиентом Microsoft. В чем вероятная причина проблемы?

3. Вы заметили, что доступ к сетевым ресурсам с Вашего компьютера Windows 2000 Server осуществляется медленнее, чем с других идентичных компьютеров Windows 2000 Server той же сети. Единственное отличие, которое Вы обнаружили, — на «медленном» компьютере установлено несколько протоколов. Как решить эту проблему, используя порядок привязки протоколов?

4. Когда клиенты DHCP пытаются продлить аренду IP-адреса?

5. Для чего может потребоваться определить на сервере DHCP несколько областей?

6. Как вручную восстановить БД DHCP?

7. Перечислите конфигурационные требования для установки сервера WINS.

8. Зачем может потребоваться несколько серверов имен?

9. Для чего создаются зоны прямого и обратного просмотра?

10. В чем разница между DNS и Dynamic DNS?

ГЛАВА 10

Служба маршрутизации и удаленного доступа

В этой главе

Служба маршрутизации и удаленного доступа (Routing And Remote Access Service, RRAS) предоставляет компьютерам Microsoft Windows 2000 Server встроенные службы сервера многопротокольной маршрутизации и *виртуальной частной сети* (VPN). RRAS появилась в Windows **NT** 4.0 Server; она позволяла превратить компьютер в промежуточный динамический программный маршрутизатор. В этой главе рассказывается о реализации RRAS в Windows 2000. Вы также узнаете о возможностях RRAS, реализации удаленного доступа, виртуальных частных сетей и об администрировании RRAS.

Прежде всего

Для выполнения заданий Вам потребуется;

- установить Windows 2000 Server на Server01 и Server02;
- установить и настроить модем на ServerOl; в процессе установки Windows 2000 Server модем может быть обнаружен автоматически, в противном случае установите ПО поддержки модема, вызвав приложение Add/Remove Hardware (Установка оборудования) из Control Panel (Панель управления).
- выполнить все упражнения предыдущих глав.

Занятие 1. Знакомство с RRAS

Поддержка многопротокольной маршрутизации для семейства ОС Windows NT появилась во втором пакете исправлений для Windows NT 3.51, включавшем компоненты протокола RIP для IP- и IPX-сетей, а также компоненты протокола SAP для IPX-сетей. Windows NT 4.0 тоже включает эти компоненты. В июне 1996 г, Microsoft выпустила RRAS для Windows NT 4.0, заменившую службу удаленного доступа Windows NT 4.0, RIP для IP, RIP для IPX и SAP для служб IPX одной интегрированной службой, обеспечивающей и удаленный доступ, и многопротокольную маршрутизацию. Занятие посвящено реализации RRAS в Windows 2000. Мы также обсудим установку и настройку этой службы, аутентификацию (проверку подлинности) и авторизацию.

Изучив материал этого занятия, Вы сможете:

- ✓ описать службу RRAS для Windows 2000;
- ✓ настроить и активизировать RRAS, используя оснастку Routing And Remote Access (Маршрутизация и удаленный доступ).

Продолжительность занятия — около 30 минут.

Служба RRAS в Windows 2000

Продолжает развитие служб многопротокольной маршрутизации и удаленного доступа для платформы Microsoft Windows. В RFAS для Windows NT 4.0 были реализованы:

- поддержка протокола RIP версии 2 для IP-сетей (протокол RIP для IP-сетей также поддерживается);
- поддержка протокола маршрутизации OSPF (Open Shortest Path First) для IP-сетей;
- маршрутизация вызова по требованию по коммутируемым каналам ГВС;
- обнаружение маршрутизаторов средствами ICMP (Internet Control Message Protocol),
- клиент RADIUS, позволяющий задействовать службы сервера RADIUS;
- сервер RADIUS, обеспечивающий централизованную аутентификацию, авторизацию, учет и политику удаленного доступа для клиентов, подключающихся по телефонной линии, и VPN-клиентов (поддержка этой функции включена в Windows NT 4.0 Option Pack);
- фильтрация пакетов IP и IPX, обеспечивающая безопасность на уровне протокола;
- средство администрирования Routing and RAS Admin с графическим интерфейсом пользователя и утилита командной строки Routemon.

RRAS для Windows 2000, основанная на RRAS Windows NT 4.0, кроме того, поддерживает:

- протокол Internet Group Management Protocol (IGMP) и многоадресную рассылку;
- трансляцию сетевых адресов при помощи компонентов адресации и разрешения имен, упрощающих подключение небольших локальных сетей к Интернету;
- встроенную маршрутизацию AppleTalk;
- протокол L2TP (Layer 2 Tunneling Protocol) поверх IPSec (IP Security) для VPN-соединений;
- усовершенствованные средства администрирования и управления: оснастку Routing And Remote Access и утилиту командной строки netsh (Net Shell);
- усовершенствованную службу IAS.

RRAS, полностью интегрированная в ОС Windows 2000 Server, поддерживает множество аппаратных платформ и сотни сетевых адаптеров. Применение RRAS выгоднее ис-

пользования промежуточного выделенного маршрутизатора или специализированного сервера удаленного доступа.

RRAS можно расширять с помощью API-интерфейсов; разработчики могут использовать их для создания собственных сетевых решений.

Комбинированные функции службы RRAS позволяют компьютеру Windows 2000 Server работать в качестве многопротокольного маршрутизатора, маршрутизатора по запросу и сервера удаленного доступа.

Многопротокольный маршрутизатор

Компьютер с RRAS способен одновременно маршрутизировать протоколы IP, IPX и AppleTalk. Все маршрутизируемые протоколы и протоколы маршрутизации настраиваются при помощи одной административной утилиты.

Маршрутизация вызова по требованию

Компьютер с RRAS может маршрутизировать протоколы IP и IPX по выделяемым (запрашиваемым) или постоянным ГВС-каналам, например, по аналоговым телефонным линиям или ISDN-каналам и по PIN-соединениям (с помощью протоколов PPTP или L2TP поверх IPSec).

Сервер удаленного доступа

Компьютер под управлением RRAS способен играть роль сервера удаленного доступа, к которому могут подключаться клиенты, соединяющиеся по телефонной линии и VPN-клиенты удаленного доступа, использующие протоколы IP, IPX, AppleTalk или NetBEUI. Совместив на одном компьютере службы маршрутизации и удаленного доступа, Вы создадите маршрутизатор удаленного доступа Windows 2000.

Совмещение служб маршрутизации и удаленного доступа

До реализации RRAS в Windows NT службы маршрутизации и удаленного доступа работали раздельно. Использование протокола PPP (Point-to-Point Protocol) позволило объединить эти службы. PPP — это пакет протоколов, применяемый для установления соединений «точка — точка» с клиентами удаленного доступа. PPP обеспечивает согласование параметров связи, обмен аутентификационными сведениями и согласование протокола на сетевом уровне. Так, при подключении к поставщику услуг Интернета по PPP согласовываются размер и разбивка на кадры пакетов (согласование на канальном уровне), Вы входите в сеть по имени пользователя и паролю (согласование аутентификации) и получаете IP-адрес (согласование на сетевом уровне).

Подключения с маршрутизацией по требованию также используют PPP для предоставления тех же служб, что и удаленные соединения (обмен параметрами связи, аутентификация и согласование на сетевом уровне). Таким образом, интеграция маршрутизации (включая маршрутизацию по требованию) и удаленного доступа позволяет компонентам удаленного доступа использовать клиент-серверную инфраструктуру протокола PPP.

Инфраструктура PPP в Windows 2000 включает поддержку:

- удаленного доступа по аналоговым телефонным линиям или линиям ISDN в качестве клиента или сервера;
- удаленного доступа к VPN в качестве клиента или сервера;
- запрашиваемой или постоянной удаленной маршрутизации по требованию по аналоговым телефонным линиям или линиям ISDN в качестве запрашивающего или отвечающего маршрутизатора;
- запрашиваемой или постоянной VPN-маршрутизации по требованию в качестве запрашивающего или отвечающего маршрутизатора.

Поддержка ЛВС и ГВС

RRAS способна работать с сетевыми адаптерами ЛВС и ГВС, поддерживаемыми Windows 2000 Server, включая платы от Eicon, Cisco, SysKonnect, Allied и US Robotics. Подробнее о поддерживаемых сетевых платах см. Windows 2000 Hardware Compatibility List на Web-узле Microsoft по адресу *http://www.microsoft.com*.

Установка и настройка

В отличие от RRAS в Windows NT 4.0 и большинства сетевых служб Windows 2000, службу RRAS не надо устанавливать или удалять с помощью Add/Remove Programs из Control Panel. RRAS автоматически устанавливается в отключенном состоянии.

Включить и настроить RRAS позволяет оснастка Routing And Remote Access (Маршрутизация и удаленный доступ). По умолчанию локальный компьютер Windows 2000 Server является сервером RRAS (рис. 10-1).

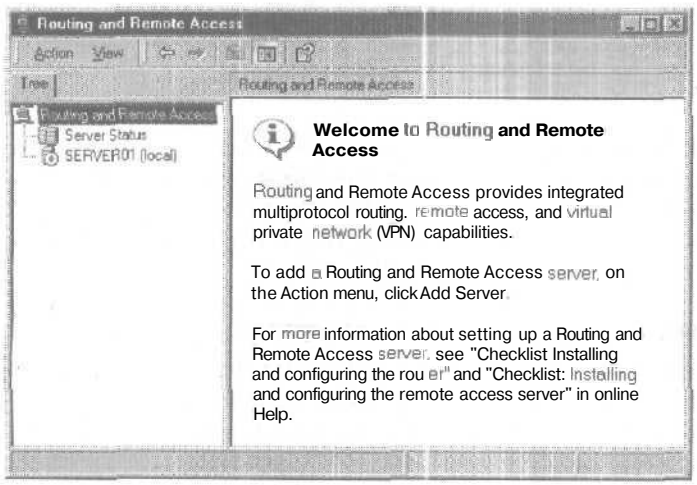


Рис. 10-1. Оснастка Routing And Remote Access (Маршрутизация и удаленный доступ) отображает отключенный сервер RRAS (локальный SERVER01)

Чтобы добавить дополнительные RRAS-серверы, щелкните корень дерева консоли или узел Server Status (Состояние сервера) и выберите в меню Action команду Add Server (Добавление сервера). Для активизации сервера, добавленного в дерево консоли, выберите нужный сервер, в меню Action (Действие) — команду Configure And Enable Routing And Remote Access (Настроить и включить маршрутизацию и удаленный доступ) и следуйте инструкциям мастера маршрутизации и удаленного доступа. По завершении работы мастера маршрутизатор удаленного доступа будет включен согласно заданным Вами параметрам.

Оснастка Routing And Remote Access и утилита командной строки netsh позволяют провести более тонкую настройку.

Примечание Вывод команды **netsh ?** (справка по работе с netsh) может не вместиться в окно сеанса MS-DOS — содержимое этого окна сеанса можно прокрутить.

Каждый компьютер интрасети, обслуживаемой RRAS-сервером, должен использовать частный IP-адрес, попадающий в один из указанных ниже диапазонов:

Блок сетевых адресов	Класс адреса
10.0.0.0 - 10.255.255.255	A
172.16.0.0 - 172.31.255.255	B
192.168.0.0 - 192.168.255.255	C

Центр Internet Assigned Numbers Authority (1ANA) специально зарезервировал эти адреса для частных сетей. Подробнее см. RFC 1918.

Упражнение 1: включение RRAS и изучение ее стандартной конфигурации

Изначально RRAS на Server01 отключена. Включите ее и изучите стандартную конфигурацию службы. В дальнейшем Вы настроите RRAS для соответствия более сложным требованиям маршрутизации и удаленного доступа. Выполняйте упражнение на ServerOl.

► Задание 1: включите службу RRAS

Включите службу RRAS на ServerOl. Сначала, вызвав Add/Remove Hardware из Control Panel, убедитесь, что на ServerOl установлен и опознан модем.

1. Зарегистрируйтесь на ServerOl как Administrator с паролем password.
2. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык Routing And Remote Access.
   Откроется окно оснастки Routing And Remote Access (Маршрутизация и удаленный доступ); в дереве консоли будет выделен узел Server01.
3. Разверните окно оснастки и прочитайте сообщение в правой панели.
4. В меню Action (Действие) выберите команду Configure And Enable Routing And Remote Access (Настроить и включить маршрутизацию и удаленный доступ).
   Откроется окно мастера настройки сервера маршрутизации и удаленного доступа.
5. Щелкните кнопку Next (Далее).
   Откроется окно Common Configurations (Обшие параметры). Настроить сервер RRAS можно пятью способами. Вы изучите их и настроите сервер RRAS как сервер удаленного доступа (сервер RAS).
6. Убедитесь, что выбран переключатель Internet Connection Server (Сервер подключения к Интернету) и щелкните кнопку Next (Далее).
   Откроется окно Internet Connection Server Setup (Установка сервера подключения к Интернету). Настроить сервер RRAS для предоставления всем компьютерам сети доступа к Интернету можно двумя способами. Первый — Internet Connection Sharing (ICS) (Установить общий доступ к подключению к Интернету) — использовать папки Network and Dial-Up Connections (Сеть удаленный доступ к сети); в окне свойств каждого удаленного соединения на вкладке Sharing (Доступ) можно настроить совместный доступ компьютеров сети к Интернету. Второй — Network Address Translation (NAT) (Установить маршрутизатор с протоколом преобразования сетевых адресов) — настроить совместный доступ с помощью мастера. NAT позволяет настроить сервер для отправки и получения пакетов из Интернета от имени клиентов интрасети. Действительный и допустимый в Интернете IP-адрес в данном случае требуется лишь оборудованию сервера RRAS.
7. Щелкните кнопку Back (Назад).
   Откроется окно Common Configurations, Прочитайте, но не выполняйте описанные в этом абзаце процедуры. Чтобы настроить сервер RRAS для обслуживания входящих

соединений, щелкните переключатель Remote Access Server (Сервер удаленного доступа). Чтобы настроить сервер для VPN-доступа (по протоколам PPTP и L2TP), щелкните переключатель Virtual Private Network (VPN) server (Сервер виртуальной частной сети). VPN позволяет клиенту удаленного доступа подключаться *к* общей сети, например к Интернету, и создает защищенное удаленное соединение с сервером RRAS. Настроить сервер RRAS для межсетевого обмена пакетами позволяет переключатель Network Router (Сетевой маршрутизатор). Чтобы вручную сконфигурировать сервер RRAS из оснастки Routing And Remote Access, щелкните переключатель Manually Configured Server (Сервер, настраиваемый вручную).

Примечание Сервер RRAS можно настроить для одновременной поддержки нескольких параметров, отображаемых в окне Common Configurations, назначение которого — помочь Вам разобраться со службой RRAS. Для дальнейшей настройки службы RRAS служат оснастка Routing And Remote Access и утилита Net Shell.

---

8. Щелкните переключатель Manually Configured Server, а затем — кнопку Next.

   Откроется окно завершения работы мастера.

9. Щелкните кнопку Finish (Готово).

   Появится сообщение, что была установлена служба маршрутизации и удаленного доступа. Вам будет предложено запустить ее.

10. **Щелкните кнопку Yes** (Да).

    Появятся сообщения Starting Routing And Remote Access (Запуск Маршрутизация и удаленный доступ) и Completing Initialization (Завершение инициализации).

► **Задание 2; изучите стандартную конфигурацию службы RRAS**

Просмотрите стандартные параметры удаленного доступа и маршрутизатора. Цель этого этапа — ознакомить Вас с функциями оснастки Routing And Remote Access.

Внимание! Не изменяйте стандартные параметры.

---

1. В дереве консоли раскройте узел Server01.

   Слева от этого узла отображается направленная вверх зеленая стрелка. Это значит, что на компьютере сконфигурирована и активна служба RRAS.

2. Раскройте меню Action (Действиг).

   Стала доступна команда Disable Routing And Remote Access (Отключить маршрутизацию и удаленный доступ), так как сервер RRAS настроен и активен.

3. Выберите команду Properties (Свойства).

   Откроется диалоговое окно свойств ServerOl.

   Параметры по умолчанию на вкладке General (Общие) указывают, что сервер настроен как маршрутизатор ЛВС и маршрутизатор по требованию, а также как сервер удаленного доступа.

4. Перейдите на вкладку Security (Безопасность).

   В качестве поставщика службы проверки пользователей и службы учета применяется Windows 2000.

5. Щелкните кнопку Authentication Methods (Методы проверки подлинности).

   Выбраны методы MS-CHAP и MS-CHAP версии 2. Для решения проблем аутентификации можно пометить флажок Allow Remote Systems To Connect Without Authentication

(Разрешить подключение удаленных систем без проверки). Выбор других способов аутентификации зависит от потребностей удаленного клиента и Ваших требований к безопасности.

6. Щелкните кнопку Cancel (Отмена) и перейдите на вкладку IP.

   Помечены флажки Enable IP Routing (Разрешить IP-маршрутизацию) и Allow IP- Based Remote Access And Demand-Dial Connections (Удаленный IP-доступ с предоставлением канала по требованию). IP-маршрутизация позволяет клиентам удаленного доступа обращаться ко всем узлам сети. Если надо, чтобы клиенты удаленного доступа обращались лишь к ресурсам сервера, сбросьте флажок Enable IP Routing. Параметр Allow IP-Based Remote Access And Demand-Dial Connections позволяет RRAS выполнять согласование IPCP (Internet Protocol Control Protocol) для PPP-подключений. Это разрешает удаленный доступ на основе IP и подключения по требованию. Вкладка IP позволяет определить порядок назначения IP-адреса (он может назначаться с помощью DHCP или выделяться из статичного пула адресов, настроенного на сервере RRAS).

7. Перейдите на вкладку PPP.

   Здесь настраиваются глобальные параметры поддержки PPP для клиентов удаленного доступа. Подробнее об этих параметрах см. занятие 3.

8. Перейдите на вкладку Event Logging (Журнал событий).

   Здесь можно определить, какие данные о событиях RRAS собирать на сервере. Для устранения неполадок щелкните переключатель Log The Maximum Amount Of Information (Вести журнал всех событий) и пометьте флажок Enable Point-To-Point Protocol (PPP) Logging (Вести журнал протокола PPP). Чтобы оптимизировать производительность сервера, щелкните переключатель Disable Event Logging (Отключить журнал событий).

9. Щелкните кнопку Cancel (Отмена).

10. В дереве консоли щелкните элемент Routing Interfaces (Интерфейсы маршрутизации).

    В правой панели появится список интерфейсов маршрутизатора. Интерфейс Loopback (Замыкание на себя) является локальным стеком протокола сервера RRAS. Local Area Connection (Подключение по локальной сети) — это сетевая плата, через которую сервер RRAS подключен к сети. Internal (Внутренний) — это функция маршрутизации в RRAS. Если маршрутизация отключена, в столбце Operational Status (Состояние) для интерфейса Internal (Внутренний) указано Non-operational (Неактивно).

11. В дереве консоли щелкните Ports (Порты).

    В правой панели отображен установленный на Вашем компьютере модем или устройство для взаимодействия с ГВС. По умолчанию для VPN используется по пять PPTP- и L2TP-минипортов. Параллельные устройства, отображаемые в правой панели, обеспечивают прямое кабельное соединение двух компьютеров. Если на Вашем компьютере есть лишь порт LPT, обозначенный как LPT1, имя прямого кабельного соединения будет указано как Direct Parallel (LPT1) [(Прямой параллельный порт (LPT1)]. Если удаленный клиент подключен к одному из портов, но производительность низка или Вы устраняете неполадки подключения, выберите порт, к которому подключен клиент, а затем в меню Action (Действие) выберите команду Status (Состояние). Появятся статистические данные о сети и информация об ошибках подключения.

12. Убедитесь, что в дереве консоли выбран узел Ports (Порты) и выберите в меню Action (Действие) команду Properties (Свойства).

    Откроется диалоговое окно Ports Properties (Свойства: Порты), где можно указать допустимое число портов каждого типа (только для VPN-подключений) и определить вид подключения через данный тип порта — только входящие или входящие и исходящие.

Кроме того, здесь можно указать номер телефона, используемый устройством доступа, Этот номер используется как *код вызываемой станции* (Called-Station-ID), а также в многоканальных подключениях по протоколу BAP (Bandwidth Allocation Protocol). Когда клиент удаленного доступа BAP запрашивает другое подключение, сервер удаленного доступа в ответ сообщает номер телефона для нового подключения. При настройке порта VPN вместо телефонного номера надо указать IP-адрес.

13. Щелкните кнопку Cancel (Отмена).
14. В дереве консоли щелкните Remote Access Clients (Клиенты удаленного доступа).

    Если удаленный клиент подключен к серверу RRAS, в правой панели появится имя подключенного пользователя, продолжительность звонка и число выделенных данному подключению портов (многоканальное подключение).
15. В дереве консоли раскройте узел IP Routing (IP-маршрутизация) и щелкните General (Общие).

    Информация в правой панели аналогична представленной на правой панели узла Routing Interfaces (Интерфейсы маршрутизации).
16. В меню Action (Действие) выберите команду New Routing Protocol (Новый протокол маршрутизации).

    Откроется одноименное диалоговое окно.

    По умолчанию отображаются протоколы NAT, OSPF и RIP версии 2 для IP. Подробнее о них см. занятие 2.
17. Щелкните кнопку Cancel (Отмена).
18. В правой панели щелкните Internal (Внутренний) и раскройте меню Action.

    Доступно множество команд для мониторинга интерфейса. Команда Properties позволяет задать общие параметры маршрутизатора для сервера RRAS.

    Просмотрите свойства интерфейсов Internal и Local Area Connection (Подключение по локальной сети) и вернитесь в оснастку Routing And Remote Access.

    Узел Static Routes (Статические маршруты) в дереве консоли, позволяющий просматривать и настраивать дополнительные маршруты к другим сетям, является графическим эквивалентом утилиты командной строки Route.

    Узел DHCP Relay Agent (Агент DHCP-ретрансляции) позволяет пересылать из одной сети в другую запросы и ответы DHCP. Благодаря этому, DHCP-сервер может предоставлять конфигурационные сведения об IP-адресе клиентам DCHP (модифицированный протокол BOOTP) и клиентам с поддержкой BOOTP, находящимся в других сетях, доступных через маршрутизатор.

    Узел IGMP позволяет сконфигурировать параметры протокола Internet Group Messaging Protocol.
19. В дереве консоли щелкните узел Remote Access Logging (Ведение журнала удаленного доступа).

Примечание Если для аутентификации и сбора информации используется сервер RADIUS, папка Remote Access Logging в дереве консоли оснастки не отображается.

    В правой панели появится элемент Local File (Локальный файл); в столбце Description (Описание) будет указан путь к папке LogFiles.
20. В правой панели дважды щелкните Local File (Локальный файл).

    Откроется диалоговое окно Local File Properties (Свойства: Локальный файл).

Вкладки Settings (Параметры) и Local File (Локальный файл) позволяют задать параметры сбора сведений; на вкладке Settings можно определить, какую информацию собирать об аутентификации, администрировании и состоянии удаленного доступа.

21. Перейдите на вкладку Local File (Локальный файл),

    Здесь можно задать формат файла журнала, время создания новых журналов, а также папку, где будут храниться файлы журналов. Папку с файлами журнала рекомендуется переместить с загрузочного раздела на какой-либо другой.
22. Щелкните кнопку Cancel (Отмена).
23. В дереве консоли щелкните узел Remote Access Policies (Политика удаленного доступа).

    В правой панели появится политика удаленного доступа по умолчанию — Allow Access If Dial-In Permission Is Enabled (Разрешить доступ, если разрешены входящие подключения).
24. Дважды щелкните Allow Access If Dial-In Permission Is Enabled.

    Откроется окно свойств этой политики.
25. Щелкните кнопку Edit (Изменить).

    Откроется диалоговое окно Time Of Day Constraints (Ограничения на время дня).

    Разрешение входящего подключения действует круглосуточно.
26. Щелкните кнопку Cancel (Отмена).

    Выбран переключатель Deny Remote Access Permission (Отказать в праве удаленного доступа) — значит, если данный профиль не переопределен для подключающегося пользователя, ему будет отказано в доступе согласно разрешениям профиля.
27. Щелкните кнопку Add (Добавить).

    Откроется диалоговое окно Select Attribute (Выбор атрибута) с параметрами подключения, которые могут быть связаны с данным профилем. Доступ предоставляется (или нет) пользователям, соответствующим условиям в профиле.
28. Щелкните кнопку Cancel (Отмена).
29. Щелкнув кнопку Edit Profile (Изменить профиль), просмотрите доступные вкладки и параметры редактирования профиля. Многие параметры профиля можно задать, не используя окно его свойств, из оснастки Routing And Remote Access.
30. Щелкните кнопку Cancel (Отмена).
31. Щелкните кнопку Cancel, чтобы закрыть окно Allow Access If Dial-In Permission Is Enabled Properties (Свойства: Разрешить доступ, если разрешены входящие подключения).
32. Сверните окно оснастки Routing And Remote Access — она понадобится в следующем упражнении.

Примечание Настроить RRAS позволяет и утилита netsh.

Отключение службы RRAS

Это можно сделать из оснастки Routing And Remote Access. Щелкните в дереве консоли компьютер, на котором надо отключить службу RRAS, и выберите в меню Action команду Disable Routing And Remote Access (Отключить маршрутизацию и удаленный доступ). При отключении RRAS из реестра удаляются все ее параметры. Отключение и повторное включение позволяет обновить параметры RRAS.

Примечание При отключении RRAS текущие параметры службы, включая конфигурацию протокола маршрутизации и интерфейсов предоставления канала по запросу, удаляются, а подключенные в данный момент клиенты — отключаются.

Аутентификация и авторизация

Зная, чем аутентификация отличается от авторизации, Вы поймете, почему попытка соединения принимается или отклоняется.

- В ходе аутентификации проверяются реквизиты пользователя при попытке подключения. Аутентификация включает передачу клиентом удаленного доступа реквизитов серверу удаленного доступа открыто или в зашифрованном виде по протоколу аутентификации.
- Авторизация — это проверка разрешения на подключение; осуществляется после успешной аутентификации.

Для успешного подключения соединение должно быть аутентифицировано и авторизовано. Может случиться, что соединение, аутентифицированное с действительными реквизитами пользователя, не будет авторизовано. При этом попытка подключения отклоняется.

Если сервер удаленного доступа настроен для аутентификации средствами Windows, система зашиты Windows 2000 проверяет аутентификационные реквизиты и параметры удаленного доступа учетной записи подключающегося пользователя; затем локальная политика удаленного доступа авторизует соединение. Аутентифицированное и авторизованное соединение будет установлено.

Если сервер удаленного доступа настроен для аутентификации средствами службы RADIUS, реквизиты подключающегося пользователя передаются серверу RADIUS для аутентификации и авторизации. Если аутентификация и авторизация прошли успешно, сервер RADIUS отсылает серверу удаленного доступа подтверждение, и тот устанавливает соединение. Если соединение не аутентифицировано или не авторизовано, сервер RADIUS сообщает об ошибке серверу RAS. и сервер удаленного доступа отклоняет соединение.

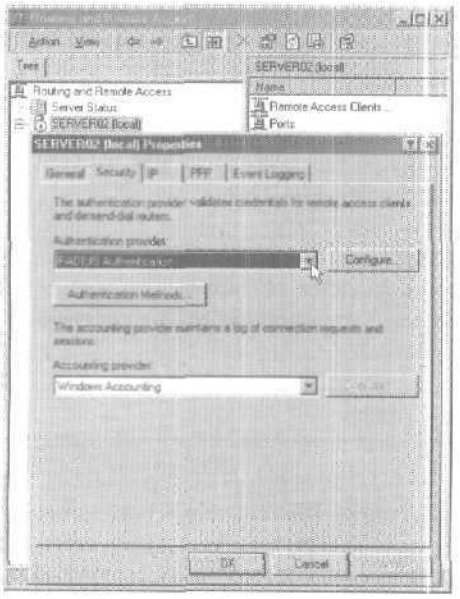


Рис. 10-2, Окно свойств сервера RRAS на Server02; в качестве средства аутентификации выбран сервер RADIUS

Если сервер RADIUS — Windows 2000-компьютер со службой IAS (Internet Authentication Service), сервер IAS осуществляет аутентификацию через систему безопасности Windows 2000. Авторизация же осуществляется согласно параметрам удаленного доступа учетной записи подключающегося пользователя, а также политики удаленного доступа, хранящейся на сервере IAS.

Выбрать поставщика службы проверки подлинности позволяют вкладка Security (Безопасность) диалогового окна свойств маршрутизатора удаленного доступа (рис. 10-2) и утилита netsh.

Резюме

Служба RRAS полностью интегрирована с Windows 2000 Server и работает с множеством аппаратных платформ и сетевых адаптеров. Комбинированные функции RRAS обеспечивают работу компьютера Windows 2000 Server в качестве многопротокольного маршрутизатора, маршрутизатора по требованию и сервера удаленного доступа. RRAS устанавливает соединения «точка — точка» с клиентами удаленного доступа по протоколу PPP, обеспечивающему согласование параметров связи, обмен аутентификационными сведениями и согласование протокола на сетевом уровне. RRAS конфигурируется, настраивается и отключается из оснастки Routing And Remote Access. Соединение должно быть аутентифицировано и авторизовано.

Занятие 2, Возможности службы RRAS

RRAS Windows 2000 поддерживает одно- и многоадресную IP-маршрутизацию, маршрутизацию протоколов IPX и AppIeTalk, удаленный доступ и VPN.

Изучив материал этого занятия, Вы сможете:

✓ описать возможности службы RRAS Windows 2000.

Продолжительность занятия — около 25 минут.

Поддержка одноадресной IP-маршрутизации

Windows 2000 обеспечивает расширенную поддержку одноадресной IP-маршрутизации (маршрутизация на один IP-адрес), используя одноадресные протоколы IP-маршрутизации и маршрутизатор Windows 2000. При одноадресной рассылке два компьютера для обмена данными устанавливают двунаправленное соединение типа «точка — точка». Одноадресной маршрутизацией называют перенаправление трафика, предназначенного для одного получателя в объединенной сети, от узла-источника к узлу-приемнику с помощью маршрутизаторов. На сложность реализации IP-маршрутизации единичных рассылок влияют:

- размер Вашей IP-сети;
- использование протокола DHCP для выделения IP-адресов;
- наличие соединения с Интернетом;
- наличие в Вашей сети узлов третьих фирм или старых узлов и др.

Ниже описаны компоненты одноадресной IP-маршрутизации.

Компонент	Описание
Статичная маршрутизация IP	Устаревшая функция протокола TCP/IP для Windows 2000, позволяет управлять статичными маршрутами из оснастки Routing And Remote Access или с помощью утилиты netsh. Утилита routemon в Windows 2000 не поддерживается
RIP версий 1 и 2	Дистанционно-векторный протокол **маршрутизации,** широко применяемый в небольших и средних по размеру IP-сетях
OSPF	Прогокол с объявлением о состоянии канала, широко используемый в средних и больших IP-сетях. OSPF гораздо эффективнее RIP, поскольку для поиска оптимального маршрута между двумя узлами применяются более совершенные алгоритмы
Агент ретрансляции DCHP	Передает DHCP-сообщения между клиентами и серверами **DHCP,** находящимися **в разных** сегментах сети. Это позволяет серверу **DHCP** обслуживать несколько областей действия. **Подробности см.** в **RFC** 1542
Трансляция сетевого адреса (NAT)	Создает транслированное соединение между сетями, использующими частные адреса, и Интернетом. Позволяет настроить домашнюю или небольшую офисную сеть на совместное использование одного подключения к Интернету

(*окончание*)

Компонент	Описание
Фильтрация IP-пакетов	Позволяет определять допустимый входящий/исходящий трафик для каждого интерфейса, основываясь на исходном и конечном IP-адресах, номерах портов TCP и UDP, видах и кодах ICMP. Является важной функцией защиты
Идентификация маршрутизаторов ICPM	Позволяет периодически распространять и отвечать на запросы узла маршрутизатора для поддержки идентификации маршрутизаторов ICMP узлами данного сегмента сети.

Поддержка многоадресной IP-маршрутизации

Windows 2000 поддерживает отправку, получение и перенаправление трафика многоадресных IP-рассылок. Трафик многоадресной рассылки передается одному узлу, но обрабатывается несколькими узлами, *перехватывающими* этот тип трафика. Обычно многоадресная IP-рассылка применяется для доставки в реальном времени данных нескольким пользователям, например, при рассылке распределенной презентации. Компоненты многоадресной IP-рассылки службы RRAS позволяют принимать и передавать трафик многоадресных рассылок от клиентов удаленного доступа, из сегментов Интернета и частных интрасетей, поддерживающих многоадресную рассылку.

Ниже описаны компоненты многоадресной IP-маршрутизации.

Компонент	Описание
Перенаправление многоадресного трафика	Устаревшая функция протокола TCP/IP для Windows 2000, позволяет просматривать таблицу перенаправления многоадресного трафика с помощью оснастки Routing And Remote Access или утилиты netsh
IGMP версий 1 и 2	Протокол пакета TCP/IP, позволяет отслеживать членство в многоадресной группе в подключенных сегментах сети
Специфическое перенаправление и маршрутизация данных	Если Вы используете протокол маршрутизации IGMP и настраиваете интерфейсы для работы в режимах маршрутизатора или прокси IGMP, маршрутизатор Windows 2000 может поддерживать перенаправление и маршрутизацию данных для специфических конфигураций
Границы многоадресной рассылки	Границы многоадресной рассылки (пределы перенаправления трафика многоадресной IP-рассылки) могут основываться на IP-адресе многоадресной группы, времени TTL, указанном в IP-заголовке, или на максимальном объеме многоадресного трафика, заданном в кб/сек

Поддержка IPX

Маршрутизатор Windows 2000 Server — полностью функциональный IPX-маршрутизатор, поддерживающий RTP для IPX (основной протокол маршрутизации, используемый в IPX-сетях), Novell NetWare SAP для IPX (протокол сбора и распространения имен и адресов служб) и перенаправление широковещательного трафика NetBIOS поверх IPX.

Ниже описаны компоненты IPX-маршрутизации.

Компонент	Описание
Фильтрация IPX-пакетов	Позволяет определять допустимый входящий/исходящий трафик для каждого интерфейса на основе фильтрации IPX-сети, узла, номеров сокетов и типа пакета
RIP для IPX	Протокол использующий дистанционно-векторный алгоритм; широко применяется в IPX-сетях. RRAS позволяет сконфигурировать также статичные IPX- и фильтры RIP-маршрутов
SAP для IPX	Протокол распространения информации, использующий дистанционно-векторный алгоритм. Широко применяется в IPX-сетях для распространения сведений о службах и их местоположении. RRAS также позволяет сконфигурировать статичные службы SAP и фильтры служб SAP. Фильтры служб уменьшают ненужный трафик, пересылаемый по RRAS-соединению
NetBIOS поверх IPX	Протокол NetBIOS поверх IPX используется сетевыми компонентами Microsoft для поддержки компонентов совместного использования файлов и принтеров. RRAS может также переправлять трафик широковещательных рассылок NetBIOS поверх IPX и позволяет настраивать статичные имена NetBIOS

Поддержка AppleTalk

RRAS может маршрутизировать протокол AppleTalk, переправляя пакеты AppleTalk и обеспечивая поддержку протокола Routing Table Maintenance Protocol (RTMP). Windows 2000 поддерживает стек протоколов AppleTalk и ПО, осуществляющее маршрутизацию AppleTalk, благодаря чему сервер Windows 2000 может подключаться и обеспечивать маршрутизацию сетей Macintosh, использующих AppleTalk.

Как и любые другие, большинство крупных сетей AppleTalk не являются непрерывными физическими сетями, в которых все компьютеры подключены к одной и той же системе кабелей. Напротив, они представляют собой объединение интрасетей AppleTalk — небольших физических сетей, соединенных маршрутизаторами.

RRAS не ограничивает количество установленных в системе сетевых адаптеров, обеспечивающих поддержку сети AppleTalk.

Маршрутизация по требованию

Windows 2000 поддерживает маршрутизацию по требованию — маршрутизацию пакетов, пересылаемых по соединениям типа «точка — точка», например, по аналоговым телефонным линиям или ISDN. Маршрутизация по запросу позволяет подключаться к Интернету, соединять офисы организации и реализовывать VPN-соединения типа «маршрутизатор — маршрутизатор».

IP- и IPX-трафик может пересылаться через запрашиваемые интерфейсы по постоянным или запрашиваемым ГВС-каналам. Для соединений по требованию RRAS автоматически создает PPP-соединение с заданным конечным узлом при приеме трафика, соответствующего статичному маршруту.

Удаленный доступ

RRAS позволяет компьютеру выступать в качестве сервера удаленного доступа, который принимает входящие соединения удаленных клиентов, применяющих традиционные средства удаленного доступа, например, аналоговые телефонные линии и ISDN. Подробнее об удаленном доступе см. занятие 3.

Сервер VPN

RRAS позволяет компьютеру выступать в качестве сервера VPN, который поддерживает PPTP и L2TP поверх IPSec и принимает удаленные VPN-соединения и VPN-соединения типа «маршрутизатор — маршрутизатор» (соединения по требованию) от клиентов удаленного доступа и вызывающих маршрутизаторов. Подробнее о VPN см. занятие 4.

Клиент-серверный протокол RADIUS

Служба Internet Authentication Service (IAS) в Windows 2000 является Microsoft-реализацией сервера RADIUS. IAS осуществляет централизованную аутентификацию, авторизацию, аудит и ведение отчетности для удаленных VPN-соединений и соединений по телефонной линии. Кроме того, IAS можно задействовать совместно с RRAS Windows 2000. IAS позволяет использовать в сети оборудование удаленного доступа и VPN-оборудование разных поставщиков.

Поставщики услуг Интернета и корпорации, предоставляющие сотрудникам удаленный доступ, сталкиваются со все усложняющейся задачей централизованного администрирования удаленного доступа независимо от применяемого оборудования. Стандарт RADIUS позволяет решить эту проблему как в однородных, так и в разнородных средах. В состав сервера удаленного доступа Windows 2000 входит клиент RADIUS, что позволяет использовать сервер удаленного доступа поставщикам услуг Интернета или организациям, применяющим RADIUS для проверки подлинности и учета. В Windows 2000 Server также входит сервер RADIUS, называемый сервером службы проверки подлинности в Интернете (IAS), который сервер удаленного доступа может задействовать как службу проверки подлинности или учета.

Сервер RADIUS обладает доступом к сведениям о пользователе и может проверять подлинность реквизитов удаленного доступа. Если реквизиты пользователя подлинны и попытка соединения авторизована, сервер RADIUS авторизует доступ пользователя в соответствии с заданными условиями и регистрирует соединения удаленного доступа как события системы учета.

Сервер RADIUS поддерживает аутентификацию и авторизацию пользователей удаленного доступа и позволяет хранить учетные данные на центральном сервере, а не на *серверах доступа к сети* (network access server, NAS). Пользователи подключаются к RADIUS-совместимому серверу NAS, например, к Windows 2000-компьютеру с установленной RRAS, который в свою очередь пересылает запросы на аутентификацию центральному серверу IAS.

Поддержка SNMP MIB

Windows 2000 и RRAS предоставляют функциональность агента SNMP с поддержкой Internet MIB II (см. RFC 1213). Станции управления сетью, например HP OpenView, могут компилировать MIB для управления событиями сетевого уровня, связанными с функциями маршрутизатора удаленного доступа Windows 2000. Чтобы станция управления сетью могла контролировать сервер RRAS, на последнем должна быть также установлена служба SNMP. Помимо Internet MIB II, для поддержки RRAS станции управления сетью могут компилировать следующие MIB:

- IP Forwarding Table MIB;
- Microsoft RIP version 2 for Internet Protocol MIB;
- Wellfleet-Series7-MIB for OSPF;
- Microsoft BOOTP for Internet Protocol MIB;
- Microsoft IPX MIB;

- Microsoft RIP and SAP for IPX MIB;
- Internet Group Management Protocol MIB;
- IP Multicast Routing MIB.

Примечание Для функций Windows 2000, устаревших функций LAN Manager MIB и служб WINS, DHCP и IIS также предусмотрена поддержка MIB. Помимо этого, служба SNMP обеспечивает поддержку протокола IPX, однако для этого должен быть установлен TCP/IP.

Поддержка компонентов сторонних фирм с помощью API-интерфейсов

Для RRAS опубликованы наборы API-интерфейсов, поддерживающих протоколы одно- и многоадресной рассылки и административные утилиты. Разработчики протоколов маршрутизации могут включить дополнительные протоколы и интерфейсы прямо в архитектуру RRAS. Прочие поставщики ПО могут использовать административные API-интерфейсы RRAS для создания собственных управляющих утилит.

Резюме

Служба RRAS для Windows 2000 поддерживает одноадресную IP-маршрутизацию (маршрутизацию сообщений, пересылаемых на один IP-адрес), а также прием, передачу и пересылку трафика многоадресных IP-рассылок. Windows 2000 может выступать как полнофункциональный IPX-маршрутизатор. RRAS поддерживает AppleTalk, маршрутизацию по требованию, удаленный доступ и VPN. Компьютер с Windows 2000 Server может выступать как сервер RADIUS и агент SNMP. Для RRAS опубликованы наборы API-интерфейсов, поддерживающих протоколы одно- и многоадресной рассылки, а также доступно множество средств администрирования.

Занятие 3. **Удаленный доступ**

Технологии удаленного доступа Windows 2000 позволяют удаленным клиентам подключаться к корпоративным сетям и к Интернету. Это занятие посвящено удаленному доступу, удаленным подключением по телефонной линии, безопасности и управлению удаленным доступом. Главное внимание уделено *службе удаленного доступа* (Remote Access Service, RAS).

Изучив материал этого занятия, Вы сможете:

- ✓ описать принципы удаленного доступа, включая подключения по телефонным линиям и обеспечение безопасности.
- ✓ управлять удаленным доступом, включая управление пользователями, адресами и аутентификацией.

Продолжительность занятия — около 35 минут.

Обзор удаленного доступа

В Windows 2000 клиенты удаленного доступа подключаются либо к ресурсам сервера удаленного доступа (соединения типа «точка — точка»), либо к ресурсам сервера RAS и ресурсам сети, в которой этот сервер находится (соединения типа «точка — ЛВС»). Соединение типа «точка — ЛВС» позволяет клиенту удаленного доступа обращаться к ресурсам так, как если бы клиент был физически подключен к сети.

Сервер RAS в Windows 2000 обеспечивает два вида удаленного доступа:

- удаленный доступ по телефонным линиям — клиент удаленного доступа использует телекоммуникационную инфраструктуру для создания временного физического канала или виртуального канала к портам сервера удаленного доступа; после создания канала производится согласование параметров подключения;
- удаленный VPN-доступ — клиент VPN использует IP-сеть для создания виртуального соединения «точка — точка» с сервером RAS, выступающим как сервер VPN; после установления подключения производится согласование его параметров.

Примечание Основное внимание в этом занятии уделено удаленному доступу по телефонным линиям; тем не менее большинство тем относятся и к удаленному доступу по VPN.

Удаленный доступ по телефонным линиям

Канал удаленного доступа по телефонным линиям включает клиент удаленного доступа, сервер удаленного доступа и инфраструктуру ГВС (рис. 10-3).

Клиент удаленного доступа

К серверу RAS Windows 2000 могут подключаться клиенты удаленного доступа Windows 2000, Windows NT 3.5 и более поздних версий, Windows 98, Windows 95, Windows for Workgroups, клиенты удаленного доступа MS-DOS и Microsoft LAN Manager, а также клиенты удаленного PPP-доступа сторонних фирм, включая клиенты UNIX и Apple Macintosh.

Клиент удаленного доступа Microsoft может подключаться к SLIP-серверу. *SLIP* (Serial Line Internet Protocol) — это старый протокол удаленного доступа, безопасность, производительность и надежность которого гораздо ниже соответствующих характеристик PPP.

Сервер RAS Windows 2000 не поддерживает удаленные SLIP-соединения по телефонным линиям.

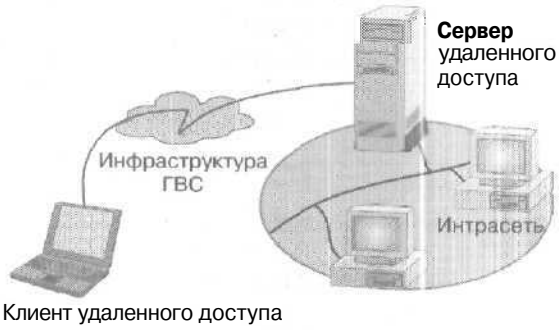


Рис. 10-3. Элементы канала удаленного доступа по телефонным линиям

Сервер удаленного доступа

Принимает удаленные подключения и пересылает пакеты между сетью, в которой он находится, и клиентами удаленного доступа.

Оборудование удаленного доступа и инфраструктура ГВС

Физическое или логическое соединение между сервером RAS и клиентом удаленного доступа создается при помощи оборудования удаленного доступа, установленного на клиентской системе, и телекоммуникационной инфраструктуры.

Коммутируемая телефонная сеть

Коммутируемая телефонная сеть общего пользования (public switched telephone network, PSTN), или *стандартная телефонная служба* (plain old telephone service, POTS), представляет собой аналоговую телефонную систему, предназначенную для передачи минимального диапазона частот, позволяющего различать голоса (рис. 10-4). Поскольку PSTN не предназначена для передачи данных, существуют ограничения на максимальную скорость двоичной передачи в битах. Оборудование удаленного доступа состоит из аналогового модема, клиента удаленного доступа и сервера RAS. В больших организациях сервер удаленного доступа подключен к пулу, содержащему сотни модемов. Если у клиента и на сервере установлены аналоговые модемы, максимальная скорость двоичной передачи в битах для соединений по PSTN составит 33 600 бит/с или 33,6 Кбит/с.

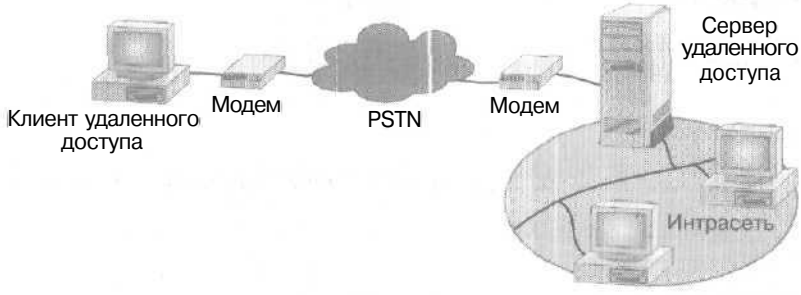


Рис. 10-4. Оборудование удаленного доступа и инфраструктура ГВС для соединений по PSTN

Цифровые линии и V.90

Максимальная скорость передачи данных по PSTN-соединению является функцией диапазона частот, передаваемых коммутаторами телефонной сети, и отношения сигнал/шум самого соединения. Современные аналоговые телефонные системы являются аналоговыми лишь на участке *локальной петли* (local loop) — комплекта проводов, соединяющих клиент с центральным коммутатором PSTN. Аналоговый сигнал, достигший коммутатора PSTN, преобразуется в цифровой. Аналогово-цифровые преобразования создают шум в соединении, или шум *квантования* (quantization).

Если сервер RAS подключен к центральному офису не через аналоговый коммутатор PSTN, а через цифровой, использующий канал типа T-Carrier или ISDN, аналогово-цифровых преобразований при передаче информации клиенту не производится. Благодаря отсутствию шума квантования повышается отношение сигнал/шум и скорость передачи. Этот новый стандарт — V.90 (рис. 10-5) — позволяет клиентам передавать данные со скоростью 33,6 Кбит/с и принимать — со скоростью 56 Кбит/с. В Северной Америке согласно правилам *Федеральной комиссии связи* (Federal Communications Commission, FCC) максимальная скорость приема — 53 Кбит/с.

Для обмена данными по стандарту V.90:

- клиент удаленного доступа должен использовать модем, поддерживающий V.90;
- сервер RAS должен использовать цифровой коммутатор стандарта V.90 и цифровой канал связи с PSTN, например T-Carrier или ISDN;
- при передаче данных от сервера RAS удаленному клиенту не должно осуществляться аналогово-цифровых преобразований.

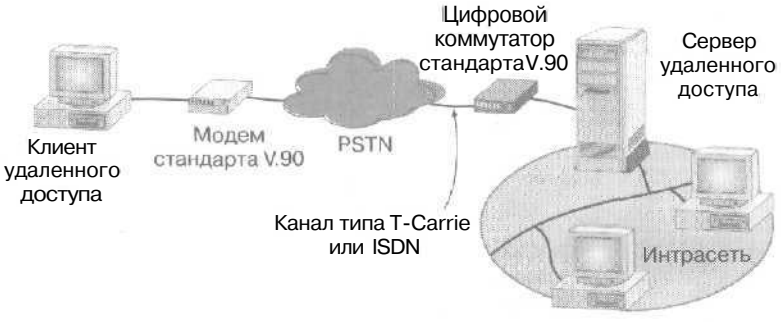


Рис. 10-5. Оборудование удаленного доступа и инфраструктура ГВС для соединений стандарта V.90

Цифровая сеть комплексных услуг

Цифровая сеть комплексных услуг (Integrated Services Digital Network, ISDN) — набор международных спецификаций по замене существующих коммутируемых телефонных сетей общего пользования — предоставляет единую цифровую сеть для передачи голоса, данных, факсов и пр. по существующей телефонной сети. ISDN аналогична телефонным линиям за исключением того, что, будучи цифровой технологией, обеспечивает высокую скорость передачи и соединения. Поскольку сеть является полностью цифровой и аналогово-цифровые преобразования не осуществляются, ISDN предлагает несколько каналов, работающих со скоростью 64 Кбит/с.

Цифровое оборудование состоит из ISDN-адаптера, установленного у клиента удаленного доступа, и сервера RAS. Клиенты обычно используют BRI-интерфейс ISDN (2 канала по 64 Кбит/с), а большие организации — PRI-интерфейс ISDN (23 канала по 64 Кбит/с). ISDN-соединение проиллюстрировано на рис. 10-6.

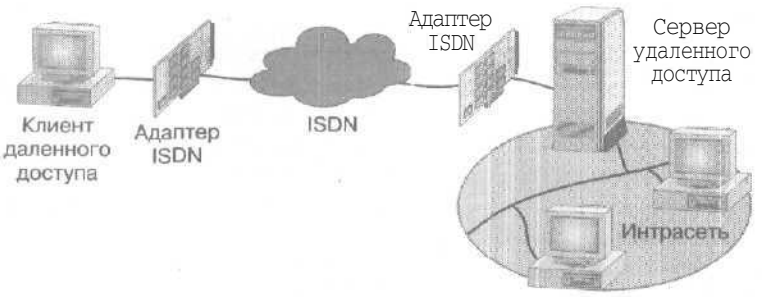


Рис. 10-6. Оборудование удаленного доступа и инфраструктура ГВС для ISDN-соединений

X.25

Это международный стандарт пересылки данных по сетям общего пользования с коммутацией пакетов (рис. 10-7). Служба RAS Windows 2000 обеспечивает поддержку X.25 двумя способами:

- клиенты удаленного доступа поддерживают работу со смарт-картами X.25, способными напрямую подключаться к сети X.25 и использовать протокол X.25 для создания соединений и передачи данных; клиенты поддерживают вызов на сборщик/разборщик пакетов несушей X.25 через аналоговый модем;
- сервер удаленного доступа Windows 2000 поддерживает лишь прямое соединение с сетью X.25 посредством смарт-карт X.25.

Рис. 10-7. Оборудование удаленного доступа и инфраструктура ГВС для соединений по стандарту X.25

Подробнее о конфигурации X.25 и сборщиках/разборщиках пакетов см. справочную систему Windows 2000 Server.

Примечание Смарт-карта X.25 — адаптер, использующий протокол X.25, — позволяет напрямую подключаться к сети данных X.25 общего пользования. Смарт-карты X.25 не связаны со смарт-картами, применяемыми для аутентификации и защиты коммуникаций.

ATM поверх ADSL

Асимметричный цифровой канал подписчика (Asymmetric Digital Subscriber Line, ADSL) - это новая технология локальной петли для небольших компаний и клиентов, работающих на дому. ADSL обеспечивает более высокую скорость передачи данных, чем PSTN- и ISDN-соединения, но скорость передачи данных к абоненту и от него различна. Стандартное ADS L-соединение обеспечивает передачу от абонента со скоростью 64 Кбит/с и к абоненту — со скоростью 1,544 Мбит/с. Будучи асимметричным, соединение идеально подходит для работы с Интернетом. Большинство пользователей Интернета получают гораздо больше информации, чем отправляют.

ADSL-оборудование может представлять собой интерфейс Ethernet или интерфейс удаленного доступа. Если адаптер ADSL является интерфейсом Ethernet, ADSL-соединение функционирует так же, как и Ethernet-соединение с Интернетом.

Если адаптер ADSL является интерфейсом удаленного доступа, ADSL обеспечивает физическое соединение, а отдельные пакеты протокола ЛВС пересылаются в *асинхронном режиме передачи* (Asynchronous Transfer Mode, ATM). Адаптер ATM с портом ADSL устанавливается на клиентской системе и на сервере удаленного доступа (рис. 10-8).

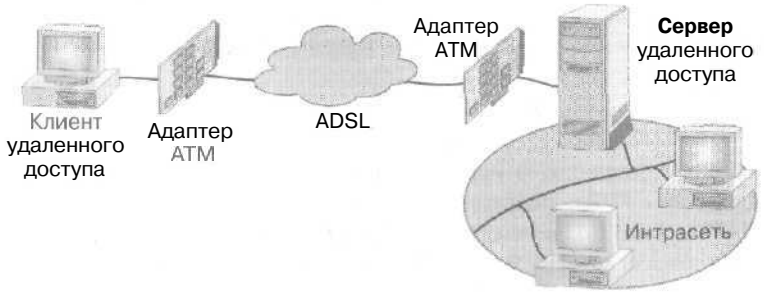


Рис. 10-8. Оборудование удаленного доступа и инфраструктура ГВС для соединений ATM поверх ADSL

Протоколы удаленного доступа

Управляют созданием соединений и передачей данных по ГВС-каналам. Протокол удаленного доступа определяется ОС и протоколами ЛВС, установленными на клиенте и на сервере.

RAS Windows 2000 поддерживает три протокола удаленного доступа:

- Point-to-Point (PPP) — промышленно стандартизированный набор протоколов, обеспечивающий наилучшие защиту, многопротокольную поддержку и возможности взаимодействия;
- Serial Line Internet Protocol (SLIP) — используется старыми серверами удаленного доступа; сервер RAS Windows 2000 не поддерживает удаленные SLIP-соединения по телефонным линиям;

- Asynchronous NetBEUI (AsyBEUI) — протокол удаленного доступа, разработанный Microsoft, используется старыми клиентами удаленного доступа, работающими под управлением ОС Microsoft, например Windows NT 3.51, Windows for Workgroups, MS-DOS и LAN Manager.

Протоколы ЛВС

Используются клиентами удаленного доступа для обращения к ресурсам сети, в которой находится сервер RAS. Служба удаленного доступа Windows 2000 поддерживает TCP/IP, IPX, AppleTalk и NetBEUI.

Защита удаленного доступа

RAS Windows 2000 предоставляет множество средств, включая безопасную аугентификацию пользователя, взаимную аутентификацию, шифрование данных, обратный вызов, номер абонента и блокировку учетной записи удаленного доступа.

Безопасная аутентификация пользователя

Достигается путем зашифрованного обмена реквизитами. Для этого совместно с PPP надо задействовать один из следующих протоколов аутентификации:

- Extensible Authentication Protocol (EAP);
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) версий 1 и 2;
- Challenge Handshake Authentication Protocol (CHAP);
- Shiva Password Authentication Protocol (SPAP).

Сервер RAS можно настроить для принудительного обеспечения безопасной аутентификации. Если клиент удаленного доступа не может обеспечить безопасную аутентификацию, подключение отклоняется.

Взаимная аутентификация

Это аутентификация обоих соединяющихся узлов путем зашифрованного обмена реквизитами пользователя. Для этого с PPP используется протокол EAP-Transport Level Security (EAP-TLS) или MS-CHAP версии 2. При взаимной аутентификации клиент удаленного доступа аутентифицирует себя для сервера RAS, а тот аутентифицирует себя для клиента удаленного доступа,

Сервер RAS может и не запрашивать аутентификацию у клиента удаленного доступа. Но если клиент удаленного доступа Windows 2000 настроен под протоколы EAP-TLS или MS-CHAP версии 2, он осуществляет принудительную аутентификацию клиента и сервера. Если сервер RAS не отвечает на запрос аутентификации, клиент разрывает соединение.

Шифрование данных

Обеспечивает кодирование информации, пересылаемой между клиентом и сервером. Шифруются лишь данные, циркулирующие по каналу связи, установленному между клиентом удаленного доступа и сервером RAS. Если Вам требуется сквозное шифрование, установите удаленное соединение и затем посредством протокола IPSec создайте зашифрованное сквозное подключение.

Примечание Протокол IPSec позволяет шифровать VPN-подключения по протоколу L2TP. Подробнее об этом см, занятие 4.

Технология шифрования удаленных подключений основана на секретном ключе, известном серверу RAS и клиенту удаленного доступа. Ключ генерируется в процессе аутентификации пользователя.

Кроме того, при совместном использовании протоколов PPP и EAP-TLS или MS-CHAP возможно шифрование данных на удаленных подключениях по телефонным линиям. Сервер RAS можно настроить для обязательного шифрования данных. Если клиент удаленного доступа не может шифровать данные, попытка подключения отклоняется.

Клиенты и серверы удаленного доступа Windows 2000/NT 4.0/98/95 поддерживают протокол Microsoft Point-to-Point Encryption (MPPE). MPPE использует поточный шифр RSA (Rivest-Shamir-Adleman) RC4 и 40-, 56- или 128-разрядные секретные ключи. Ключи MPPE генерируются на основе процессов аутентификации пользователя по протоколам EAP-TLS и MS-CHAP.

Обратный вызов

Технология *обратного вызова* (callback) позволяет серверу RAS дозваниваться до клиента после проверки реквизитов пользователя. Обратный вызов конфигурируется на сервере, чтобы сервер мог вызывать клиента по указанному им номеру. Таким образом, мобильный пользователь может дозваниваться до сервера, и тот будет вызывать пользователя по номеру, занимаемому им в текущий момент; это позволит сэкономить на оплате телефонных переговоров. Обратный вызов можно настроить и так, чтобы сервер всегда дозванивался до клиента удаленного доступа по определенному номеру. Это безопасная форма обратного вызова.

Номер абонента

Указывается в параметрах вызова учетной записи пользователя и гарантирует, что входящие звонки будут приниматься лишь с определенных телефонных номеров. Если номер дозванивающегося абонента не соответствует заданным номерам, попытка подключения отклоняется.

Для использования номера абонента телефонная линия клиента, телефонная система, телефонная линия сервера удаленного доступа и драйверы оборудования удаленного доступа Windows 2000 должны поддерживать данную функцию. Если для пользовательской учетной записи указан номер абонента и клиент не передает его серверу удаленного доступа, попытка подключения отклоняется.

Номер абонента позволяет обеспечить высокую степень зашиты для сетей с поддержкой удаленного доступа. Недостаток использования номеров абонентов в том, что клиент должен всегда подключаться по одной и той же телефонной линии. Таким же недостатком обладает функция обратного вызова, сконфигурированная для вызова по определенному номеру.

Блокировка учетных записей удаленного доступа

Позволяет отказать удаленному пользователю в доступе, если его действительная учетная запись определенное число раз не пройдет аутентификацию. Блокировка учетных записей удаленного доступа особенно важна для VPN-подключений через Интернет. Злоумышленник из Интернета может попытаться получить доступ к интрасети организации, послав при аутентификации VPN-подключения некоторые реквизиты (действительное имя пользователя и предполагаемый пароль). При атаке по словарю хакер может отсылать сотни и тысячи реквизитов, используя список паролей, состоящий из распространенных слов или фраз. Если блокировка учетных записей удаленного доступа включена, после определенного числа попыток аутентификации атака по словарю будет остановлена.

Функция блокировки учетных записей удаленного доступа не делает различий между злоумышленниками, пытающимися проникнуть в интрасеть, и настоящими пользователями, забывшими пароль. Забывчивые пользователи обычно пытаются зарегистрироваться в системе, указывая разные пароли. После превышения допустимого числа попыток их учетные записи будут заблокированы.

Включение блокировки учетных записей удаленного доступа может привести к тому, что злоумышленник непреднамеренно заблокирует учетную запись в результате попыток пройти аутентификацию, и действительный владелец учетной записи не сможет зарегистрироваться в системе.

Сетевой администратор должен определить два следующих параметра.

- Допустимое число попытокаутентификации перед блокировкой учетной записи. С каждой неудавшейся попыткой растет счетчик неудачных попыток аутентификации. По достижении максимума учетная запись удаленного доступа блокируется: Если же счетчик еще не достиг максимального значения и аутентификация прошла успешно, счетчик сбрасывается. Иначе говоря, после успешной аутентификации отсчет неудачных попыток начинается заново.
- Периодичность сброса счетчика неудачных попыток. Для предотвращения неумышленной блокировки учетных записей в результате ошибок при вводе паролей счетчик неудачных попыток следует периодически обнулять.

Управление удаленным доступом

При управлении удаленным доступом надо учесть множество факторов, например место хранения учетных записей, порядок присвоения адресов клиентам удаленного доступа и кому разрешено устанавливать удаленные подключения. Управление удаленным доступом включает управление пользователями, адресами, доступом и аутентификацией.

Управление пользователями

Вместо хранения нескольких учетных записей для одного пользователя на отдельных серверах и попыток синхронизации этих записей администраторы создают в хранилище Active Directory сервера RADIUS главную БД учетных записей. Это позволяет серверу удаленного доступа отсылать аутентификационные реквизиты центральному аутентифицирующему устройству.

Управление адресами

При установлении PPP-соединений удаленному клиенту необходимо предоставить сведения об IP-, IPX- или AppleTalk-адресе. Сервер RAS Windows 2000 следует настроить для предоставления IP-адресов, IPX-адресов сетей и узлов или AppleTalk-адресов сетей и узлов.

Управление доступом

В Windows 2000 подключение удаленного доступа принимаются на основе параметров вызова учетной записи пользователя и политики удаленного доступа — наборе условий и параметров, определяющих характеристики входящего подключения и накладываемые на него ограничения. Например, политика удаленного доступа позволяет ограничить максимальное время сеанса, определить время простоя перед отключением, указать методы безопасной аутентификации, тип шифрования и т. д.

При наличии нескольких политик доступа к разным клиентам удаленного доступа могут применяться разные наборы условий; кроме того, на основе параметров устанавли-

ваемого подключения к одному и тому же клиенту удаленного доступа могут применяться разные требования. Наличие нескольких политик удаленного доступа позволяет:

- предоставлять или отклонять подключения на основе принадлежности учетной записи пользователя к определенной группе;
- задать разные дни и время подключения для учетных записей пользователей, относящихся к разным группам;
- сконфигурировать для клиентов удаленного доступа по телефонным линиям и клиентов удаленного VPN-доступа разные методы аутентификации;
- настроить для PPTP- и L2TP-подключений аутентификацию и шифрование;
- определить для разных пользователей разные максимальные сроки сеанса на основе принадлежности учетной записи к определенной группе;
- пересылать клиенту RADUIS специфичные для NAS атрибуты RADIUS.

Если у Вас несколько серверов удаленного доступа Windows 2000 или VPN-серверов, для которых Вы хотите использовать централизованный набор политик доступа, можно установить на одном из Windows 2000-компьютеров службу IAS и настроить каждый сервер удаленного доступа или VPN-сервер в качестве клиента RADIUS для сервера IAS,

Службы RRAS Windows 2000 и IAS Windows 2000 используют политику удаленного доступа для предоставления/отклонения подключения. Администрирование политики удаленного доступа службы RRAS осуществляется из оснастки Routing And Remote Access. Для администрирования политик удаленного доступа серверов IAS служит оснастка Internet Authentication Service (Служба проверки подлинности в Интернете).

Политика удаленного доступа позволяет предоставлять подключения, конфигурируя отдельные учетные записи пользователей или отдельные политики удаленного доступа.

Доступ по учетным записям

Учетная запись пользователя изолированного сервера или сервера с Active Directory включает группу параметров вызова, применяемых при предоставлении/отклонении подключения. Чтобы настроить параметры вызова учетной записи пользователя изолированного сервера, в оснастке Local Users and Groups (Локальные пользователи и группы) откройте диалоговое окно свойств учетной записи и перейдите на вкладку Dial-In (Входящие звонки). Чтобы настроить параметры вызова учетной записи пользователя сервера Active Directory, в оснастке Active Directory Users and Groups откройте диалоговое окно свойств учетной записи и перейдите на вкладку Dial-In (рис. 10-9).

На вкладке Dial-In доступны параметры Remote Access Permission (Dial-In or VPN) [Разрешение на удаленный доступ (VPN или модем)], Verify Caller ID (Проверять идентификатор), Callback Options (Ответный вызов сервера), Assign A Static IP Address (Статический IP-адрес пользователя) и Apply Static Routes (Использовать статическую маршрутизацию).

Примечание Для учетных записей пользователей доменов Windows NT 4.0 и доменов Windows 2000 смешанного режима доступен лишь параметр Deny Access в группе Remote Access Permission (Dial-In or VPN) и параметры группы Callback Options.

Группа Remote Access Permission (Dial-In or VPN)

Переключатели этой группы позволяют явно предоставить/заблокировать доступ и указать, что предоставлением доступа управляет политика удаленного доступа. Если доступ предоставлен явно, он по-прежнему может блокироваться настройками политики удаленного доступа, свойствами учетной записи пользователя или свойствами профиля. Переключатель Control Access Tbrough Remote Access Policy (Управление на основе политики удаленного доступа) применим только для учетных записей пользователей домена Windows

2000 основного режима локальных учетных записей изолированных серверов удаленного доступа Windows 2000.

По умолчанию для учетных записей Administrator и Guest изолированного сервера удаленного доступа или домена Windows 2000 основного режима выбран переключатель Control Access Through Remote Access Policy, а для учетных записей домена Windows 2000 основного режима — переключатель Deny Access (Запретить доступ). Для новых учетных записей, создаваемых на изолированном сервере RAS или в домене Windows 2000 основного режима, также выбирается переключатель Control Access Through Remote Access Policy. Для новых учетных записей, создаваемых в домене Windows 2000 смешанного режима, выбирается Deny Access.

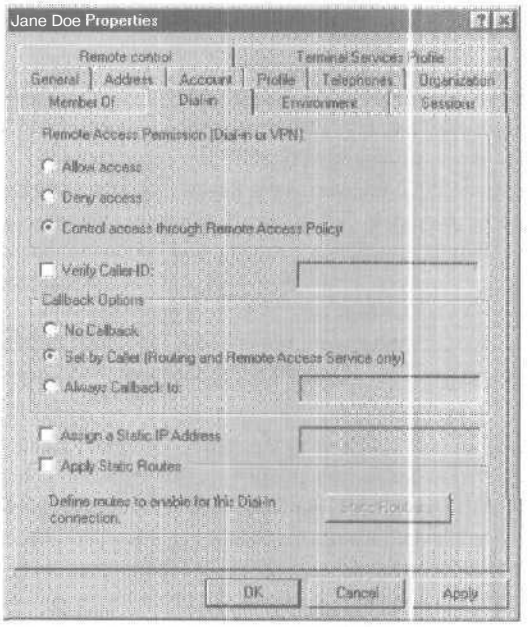


Рис. 10-9. Параметры вызова для пользователя Jane Doe

Флажок** Verify **Caller ID

При помеченном флажке сервер проверяет телефонный номер абонента. Если номер абонента не соответствует заданному, соединение отклоняется.

Передача номера абонента должна поддерживаться абонентом и телефонной сетью между абонентом и сервером удаленного доступа. На сервере требуется наличие отвечающего на звонки оборудования, которое поддерживает передачу номера абонента, и соответствующего драйвера Windows 2000, который поддерживает передачу номера абонента серверу RAS.

Если для пользователя настроен телефонный номер абонента и клиентская система не поддерживает передачу этого номера серверу удаленного доступа, попытка подключения отклоняется.

*Группа **Callback Options***

При обратном вызове сервер в процессе подключения вызывает абонента по указанному им телефонному номеру или по номеру, заданному администратором сети.

Если учетная запись пользователя относится к домену Windows 2000 основного режима, длина номера обратного вызова может составлять до 128 символов. Если же она отно-

сится к изолированному серверу удаленного доступа Windows 2000, домену Windows NT 4.0 или домену Windows 2000 смешанного режима, длина номера обратного вызова может составлять от 24 до 48 символов. Это связано с тем, что для хранения номеров используется сжатый формат. Длинные телефонные номера могут применяться для международных звонков или звонков с дополнительными кодами, например номерами телефонных карт.

Флажок Assign a Static IP Address

При помеченном флажке подключившемуся пользователю можно назначить статический IP-адрес.

Флажок Apply Static Routes

При помеченном флажке можно определить наборы статичных IP-маршрутов, добавляемых при установлении соединения в таблицу маршрутизации сервера удаленного доступа. Данный параметр предназначен для учетных записей, используемых маршрутизаторами Windows 2000 для маршрутизации по требованию.

Доступ на основе политики

Предназначен для изолированных серверов RAS Windows 2000, а также для серверов RAS — членов домена Windows 2000 основного режима. Чтобы доступ предоставлялся на основе политики, выберите на вкладке Dial-In диалогового окна свойств всех учетных записей пользователей переключатель Control Access Through Remote Access Policy (рис. 10-9). После этого определите новые политики удаленного доступа, предоставляющие/отклоняющие доступ в соответствии с Вашими требованиями. Настройка политики удаленного доступа осуществляется через поставщика службы проверки подлинности RRAS или RADIUS. На рис. 10-10 показан узел Remote Access Policy (Политика удаленного доступа) в оснастке Routing And Remote Access.

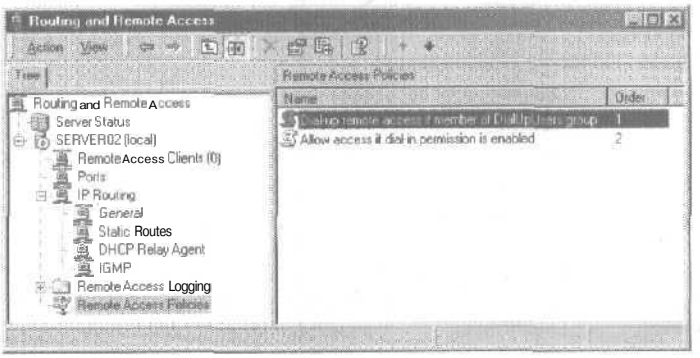


Рис. 10-10. Узел **Remote Access Policy (Политика удаленного доступа) в оснастке Routing And Remote Access (Маршрутизация и удаленный доступ); в правой панели отображаются две политики удаленного** доступа

Узел Remote Access Policy отображается в дереве консоли оснастки Routing And Remote Access, только если поставщиком проверки подлинности является Windows. Если же эту роль играет сервер RADIUS (рис. 10-2), этот узел в дереве консоли не отображается. Политики удаленного доступа настраиваются через интерфейс поставщика служб проверки подлинности RADIUS.

Если сервер RAS относится к домену Windows NT 4.0 или домену Windows 2000 смешанного режима и Вам нужно, чтобы доступ предоставлялся на основе политики, выберите на вкладке Dial-In диалогового окна свойств всех учетных записей пользователей переключатель Allow Access (Разрешить доступ). Затем удалите политику по умолчанию Allow

Access If Dial-In Permission Is Enabled (Разрешить доступ, если разрешены входящие подключения) и создайте новую, предоставляющую/отклоняющую доступ. Подключение, не соответствующее ни одной из политик удаленного доступа, отклоняется, даже если для учетной записи пользователя выбран переключатель Allow Access.

Обычно политика удаленного доступа применяется для предоставления доступа на основании принадлежности к группе. Например, создайте группу Windows 2000 с именем DialUpUsers, члены которой могут устанавливать удаленные соединения по телефонным линиям.

Чтобы создать сервер RAS, принимающий лишь удаленные подключения по телефонным линиям, создайте новую политику удаленного доступа с понятным именем, например Dial-Up Remote Access If Member of DialUpUsers group, и включите в нее группу DialUpUsers. Затем удалите политику удаленного доступа по умолчанию Allow Access If Dial-In Permission Is Enabled.

Принятие попытки подключения

Устанавливаемое подключение принимается/отклоняется согласно следующей логике (рис. 10-11).

1. Проверяется первая политика из упорядоченного списка политик удаленного доступа. Если политик удаленного доступа нет, попытка подключения отклоняется.
2. Если все условия политики не соответствуют параметрам устанавливаемого подключения, переходим к следующей политике. Если политик удаленного доступа больше нет, попытка отклоняется.
3. Если все условия политики соответствуют параметрам устанавливаемого подключения, проверяем разрешение на удаленный доступ:
   - если его нет, попытка подключения отклоняется;
   - если есть, проверяются свойства учетной записи и свойства профиля:
     - если устанавливаемое подключение не соответствует параметрам свойств учетной записи и профиля, попытка отклоняется;
     - если устанавливаемое подключение соответствует параметрам свойств учетной записи и профиля, попытка принимается.
   - При разрешении ControlAccess Through Remote Access Policy проверяется, есть ли разрешение на удаленный доступ, определенное в политике:
     - нет — попытка подключения отклоняется;
     - да — проверяются свойства учетной записи и профиля.
   - Если устанавливаемое подключение не соответствует параметрам свойств учетной записи пользователя и свойств профиля, попытка отклоняется.
   - Если устанавливаемое подключение соответствует параметрам свойств учетной записи пользователя и свойств профиля, попытка принимается.

Управление блокировкой учетных записей

Блокировка учетных записей осущес гвляется путем редактирования реестра Windows 2000-компьютера, обеспечивающего аутентификацию. Если сервер RAS сконфигурирован для аутентификации средствами Windows, отредактируйте реестр компьютера, на котором установлен сервер удаленного доступа. Если сервер RAS сконфигурирован для аутентификации средствами RADIUS и используется служба IAS Windows 2000, отредактируйте реестр сервера IAS.

Чтобы включить блокировку учетных записей, задайте параметру MaxDenials значение 1 или больше. Он находится в разделе реестра HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout и задает максимальное число неудачных попыток аутентификации перед блокировкой записи. По умол-

чанию значение MaxDenials равно 0, т. е. учетные записи не блокируются. Раздел реестра AccountLockout создается при включении службы RRAS.

Чтобы изменить периодичность сброса счетчика неудачных попыток, измените значение параметра ResetTime (Mins), находящегося в разделе реестра HKEY_LOCAL_MACHINE\SYS=TEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout. По умолчанию значение ResetTime (Mins) равно шестнадцатеричному значению b40 или, в десятичной системе единиц, 2880 минутам (48 часам).

Чтобы вручную освободить заблокированную учетную запись до сброса счетчика неудачных попыток, удалите подраздел реестра HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout\<*имя_ домена:имя_пользователя*>.

Примечание Функция блокировки учетной записи удаленного доступа не связана ни с флажком Account is locked out (Заблокировать учетную запись) на вкладке Account (Учетная запись) диалогового окна свойств учетной записи пользователя, ни с блокировкой учетных записей в групповых политиках Windows 2000.

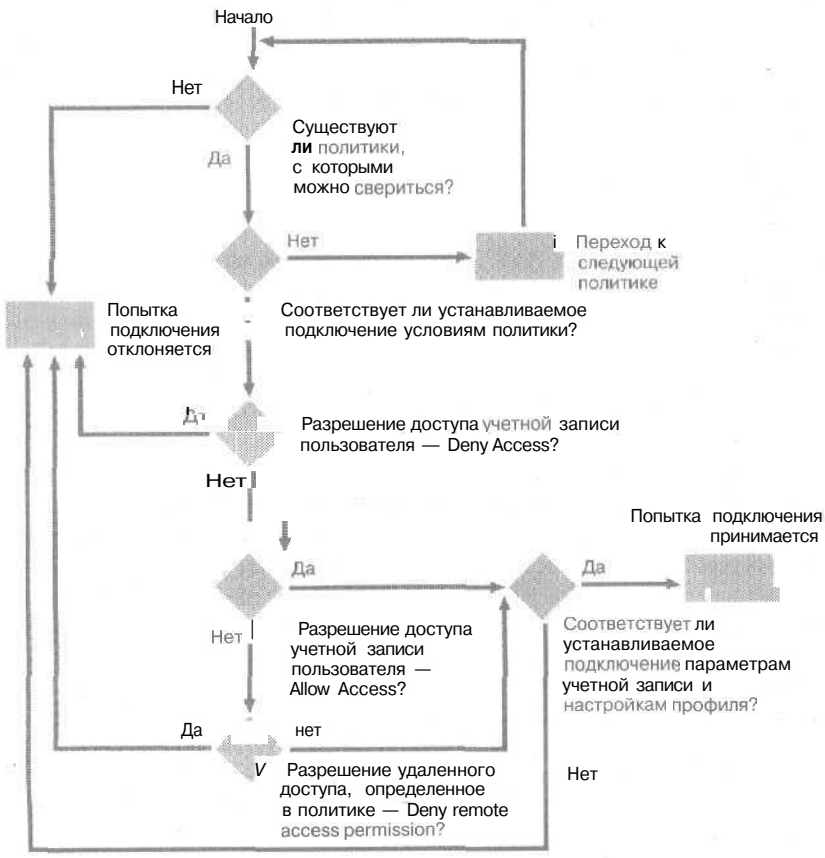


Рис. 10-11. Логика принятия подключения на основе политик удаленного доступа и параметров учетной записи пользователя

Управление аутентификацией

Сервер удаленного доступа можно настроить для аутентификации средствами Windows или RADIUS. На рис. 10-2 показано, как в оснастке Routing And Remote Access указать источник аутентификации.

Проверка подлинности средствами Windows

Если поставщиком служб проверки подлинности является Windows, аутентификация реквизитов пользователей, устанавливающих удаленные соединения, производится обычными средствами Windows.

Если сервер RAS состоит в домене Windows 2000 смешанного или основного режима и сконфигурирован для аутентификации средствами Windows, учетная запись компьютера сервера RAS должна состоять в группе безопасности RAS And IAS Servers (Серверы RAS и IAS). Администратор домена может в оснастке Active Directory Users And Computers добавить нужный сервер в группу безопасности RAS And IAS Servers в контейнере Users. Кроме того, добавить нужный сервер RAS в данную группу позволяет netsh. Например, чтобы добавить сервер RAS1 в группу безопасности RAS And IAS Servers домена microsoft.com, откройте окно сеанса MS-DOS и введите netsh. Затем наберите add **registeredserver domain=microsoft.com server=ras1**. Если устанавливающий службу RRAS пользователь — администратор, то при установке службы учетная запись компьютера автоматически добавляется в группу безопасности RAS And IAS Servers.

Проверка подлинности средствами RADIUS

Если поставщиком служб проверки подлинности является RADIUS, реквизиты пользователя и параметры запроса подключения пересылаются в виде серий запросов RADIUS серверу RADIUS, например, компьютеру Windows 2000 Server, на котором установлена служба IAS.

Сервер RADIUS получает от сервера RAS запрос пользователя на установление подключения и аутентифицирует клиента по своей БД, Кроме того, сервер RADIUS может поддерживать центральную БД других сопутствующих параметров учетной записи пользователя. В дополнение к ответу «да» или «нет» на запрос об аутентификации сервер RADIUS может сообщать серверу удаленного доступа дополнительные параметры подключения, применимые к данному пользователю, например максимальное время сеанса, статичный IP-адрес и др.

Сервер RADIUS может осуществлять аутентификацию на основе собственной БД или выступать в качестве интерфейса другого сервера БД, например стандартного ODBC-сервера или контроллера домена Windows 2000. Контроллер домена может находиться на одном компьютере с сервером RADIUS или на другой машине. Сервер RADIUS может также выступать для удаленного сервера RADIUS в качестве прокси-клиента.

О протоколе RADIUS см. RFC 2138 и RFC 2139. О сценариях аутентификации сервера RAS и работе сервера удаленного доступа в качестве клиента RADIUS см. справочную систему Windows 2000.

Примечание При аутентификации средствами Windows службы RRAS и IAS используют один процесс для аутентификации и авторизации поступающих запросов на подключение.

Учет Windows и RADIUS

На вкладке Security (Безопасность) диалогового окна свойств сервера удаленного доступа можно также указать средства ведения учета — он может вестись средствами Windows, RADIUS или не вестись вовсе. Если учет ведется средствами Windows, сервер RAS Windows 2000 поддерживает для удаленных подключений регистрацию учетной информации в ло-

кальные файлы. Регистрация событий удаленных подключений осуществляется отдельно от регистрации событий, заносимых в журнал System Log (Журнал системы). Регистрация учетной информации особенно полезна для устранения неполадок политик удаленного доступа. Учетные сведения хранятся в настраиваемых файлах журнала, размещаемых в папке %systemroot%\System32\LogFiles. Формат файлов журнала — IAS 1.0 или ODBC, т. е. любая программа для работы с БД может напрямую считывать файл для последующего анализа.

Кроме того, если аутентификация и учет осуществляются средствами RADIUS, сервер RAS Windows 2000 поддерживает для удаленных подключений регистрацию учетной информации в файлы, размещаемые на сервере RADIUS. Регистрация событий удаленных соединений осуществляется отдельно от регистрации событий, заносимых в журнал System Log. Если сервер RADIUS является компьютером Windows 2000 со службой IAS, учетная информация заносится в файлы журнала, размещаемые на сервере IAS.

Упражнение 2: настройка и мониторинг соединения удаленного доступа

► Задание 1: предоставьте и отклоните удаленный доступ по телефонной линии

Избирательно предоставьте или заблокируйте доступ для учетных записей пользователей. Выполняйте задание на Server01.

1. Откройте оснастку Active Directory Users And Computers.
2. В дереве консоли щелкните ОП Sales.
   В правой панели отобразятся объекты ОП Sales.
3. Дважды щелкните учетную запись Jane Doe.
   Откроется диалоговое окно Jane Doe Properties (Свойства: Jane Doe).
4. Перейдите на вкладку Dial-In (Входящие звонки).
   На вкладке Dial-In отображаются параметры вызова для пользователя Jane Doe.
5. Щелкните переключатель Allow Access (Разрешить доступ), а затем — OK.
6. В правой панели дважды шелкните учетную запись John Smith и перейдите на вкладку Dial-In.
   На вкладке Dial-In отображаются параметры вызова для пользователя John Smith.
7. Убедитесь, что выбран переключатель Control Access Through Remote Access Policy (Управление на основе политики удаленного доступа) и шелкните OK.
8. В дереве консоли щелкните контейнер Users.
   В правой панели появятся элементы данного контейнера.
9. Просмотрите параметры вызова для пользователя Bob Train.
10. Щелкните переключатель Deny Access (Запретить доступ), а затем — кнопку OK.
11. Закройте оснастку Active Directory Users And Computers.

► Задание 2: включите проверку подлинности и настройте протоколирование на сервере RRAS

Включите проверку подлинности средствами Windows и настройте протоколирование на сервере RRAS. Выполняйте задание на ServerOl.

1. Восстановите окно оснастки Routing And Remote Access.
2. В дереве консоли щелкните папку Remote Access Logging (Ведение журнала удаленного доступа).
3. На правой панели дважды щелкните элемент Local File (Локальный файл).
   Откроется диалоговое окно Local File Properties (Свойства: Локальный файл).

4. Пометьте флажок Log Authentication Requests (Записывать запросы проверки подлинности).
5. Щелкните кнопку OK.
6. В дереве консоли щелкните узел Server01(Local) [Server01 (локально)].
7. В меню Action (Действие) выберите команду Properties (Свойства).

   Откроется диалоговое окно свойств ServerOl.
8. Перейдите на вкладку Event Logging (Журнал событий).
9. Щелкните переключатель Log The Maximum Amount Of Information (Вести журнал всех событий) и пометьте флажок Enable Point-To-Point Protocol (PPP) Logging (Вести журнал протокола PPP).
10. Щелкните кнопку **OK.**

    Вам предложат перезапустить маршрутизатор.
11. Щелкните кнопку Yes (Да).

    При перезапуске службы марушртизации и удаленного доступа появится несколько сообщений.

► **Задание 3 (необязательное): настройте клиент удаленного доступа ло телефонной линии и подключитесь к серверу RRAS**

Настройте Server02 в качестве клиента удаленного доступа по телефонной линии. Для выполнения упражнения на Server02 должен быть установлен модем.

1. Перед включением Server02 отсоедините сетевой кабель.
2. Запустите Server02.
3. В окне регистрации в системе выберите в списке Logon To пункт SERVER02 (This Computer) и затем войдите в систему как Administrator с паролем password.
4. Раскройте меню Start\Settings (Пуск\Настройка) и выберите Network And Dial-up Connections (Сеть и удаленный доступ к сети).

   Откроется одноименное окно. Против Local Area Connection (Подключение по локальной сети) отображается красный значок «X». Приступив к заданию, Вы разорвали это подключение.
5. Дважды щелкните значок Make New Connection (Создание нового подключения).

   Откроется окно мастера создания сетевого подключения.
6. Щелкните кнопку Next (Далее).

   Откроется окно Network Connection Type (Тип сетевого подключения).
7. Убедитесь, что выбран переключатель Dial-Up To Private Network (Телефонное подключение к частной сети), и щелкните кнопку Next (Далее).

   Откроется окно Phone Number To Dial (Введите телефонный номер),
8. Если подключиться к серверу RRAS можно, укажите номер телефона, на котором установлен модем севера RRAS. Если сервер RRAS недоступен, укажите любой телефонный номер.
9. Щелкните кнопку Next (Далее).

   Откроется окно Connection Availability (Доступность подключения).
10. Щелкните кнопку Next.

    Откроется окно Internet Connection Sharing (Общий доступ к подключению Интернета).
11. Щелкните кнопку Next.

    Откроется окно Completing The Network Connection Wizard (Завершение работы мастера создания сетевого подключения). Будет создано соединение с именем по умолчанию — Dial-Up Connection (Подключение удаленного доступа).
12. Щелкните кнопку Finish (Готово).

Откроется диалоговое окно Connect Dial-up Connection (Подключение к Подключение удаленного доступа).

13. Если Вы не можете дозвониться до сервера RRAS, щелкните кнопку Cancel (Отмена). На следующем этапе будут приведены снимки экрана, на которых Вы увидите, что происходит при установлении подключения. Если Вы дозвонились до сервера RRAS, продолжайте дальше.
14. В поле User Name (Пользователь) введите Bob_Train (обратите внимание на символ подчеркивания) и щелкните кнопку Dial (Вызов).

    Появится сообщение, что у данной учетной записи пользователя нет разрешений на удаленное подключение по телефонной линии. Учетной записи пользователя Bob Train было присвоено разрешение Deny Remote Access Permission.
15. В поле User Name (Пользователь) введите **Jane_Doe**, в поле password — student и щелкните кнопку Dial (Вызов).

    На Server02 появится сообщение Connecting Dial-Up Connection (Установка связи с Подключение удаленного доступа), и подключение будет проверено, аутентифицировано и зарегистрировано.

    На Server02 появится сообщение об установлении подключения.
16. Пометьте флажок Do Not Display This Message Again (Не показывать это сообщение в дальнейшем) и щелкните кнопку OK.

    Пользователь Jane Doe успешно подключился к серверу RAS, поскольку для данной учетной записи было сконфигурировано разрешение Allow Access (Разрешить доступ).
17. В окне Network And Dial-up Connections (Сеть и удаленный доступ к сети) дважды щелкните значок Dial-up Connection (Подключение удаленного доступа к сети).

    Откроется окно Dial-Up Connection Status (Состояние Подключение удаленного доступа).
18. Щелкните кнопку Disconnect (Отключить).
19. Дважды щелкните значок Dial-up Connection (Подключение удаленного доступа к сети).
20. В поле User Name (Пользователь) введите **John_Smith** (между первым и вторым именем стоит символ подчеркивания) и шелкните кнопку Dial (Вызов).

    Появится сообщение, что у данной учетной записи пользователя нет разрешений на удаленное подключение по телефонной линии. Учетной записи пользователя Bob Train было присвоено разрешение Control access through Remote Access Policy (Управление на основе политики удаленного доступа).
21. На Server01 восстановите окно оснастки Routing And Remote Access.
22. В дереве консоли шелкните узел Remote Access Policies (Политики удаленного доступа).
23. В правой панели дважды щелкните политику Allow Access If Dial-In Permission Is Enabled (Разрешить доступ, если разрешены входящие подключения).

    Откроется диалоговое окно свойств политики.
24. В группе If A User Matches The Conditions (Если пользователь соответствует условиям) шелкните переключатель Grant Remote Access Permission (Предоставить право удаленного доступа) и щелкните кнопку OK.
25. Вернитесь к компьютеру Server02.
26. Щелкните кнопку Dial (Вызов), чтобы еще раз подключиться с учетной записью John Smith.

    Политика удаленного доступа по умолчанию предоставляет доступ всем учетным записям пользователей, на вкладке Dial-In (Входящие звонки) окна свойств которых выбран переключатель Control Access Through Remote Access Policy.

► **Задание 4 (необязательное): проведите мониторинг удаленного подключения**

Это задание можно выполнить, лишь подключившись к серверу удаленного доступа. Если Вы не смогли подключиться, здесь приводятся важные снимки экранов. Выполняйте задание на Server01.

1. Восстановите окно оснастки Routing And Remote Access.
2. Щелкните в дереве консоли элемент Remote Access Clients (1) [Клиенты удаленного доступа (1)].

   В столбце User Name (Имя пользователя) появится надпись MICROSOFT\John_Smith. Также отображаются продолжительность подключения и номера занятых портов (рис. 10-12).

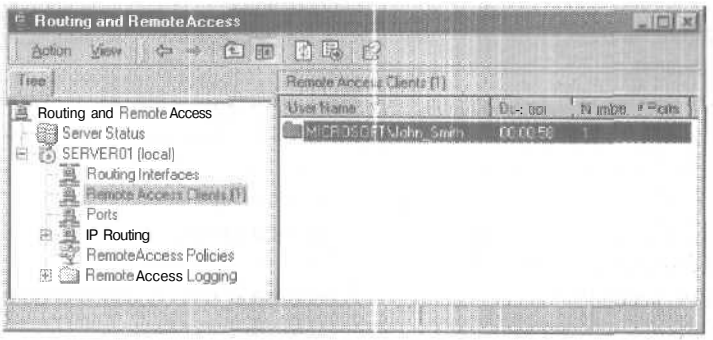


Рис. 10-12. В правой панели отображаются имя пользователя, продолжительность подключения и занимаемые порты

3. В правой панели дважды щелкните элемент MICROSOFT\John_ Smith. Откроется диалоговое окно Status (Состояние) (рис. 10-13).

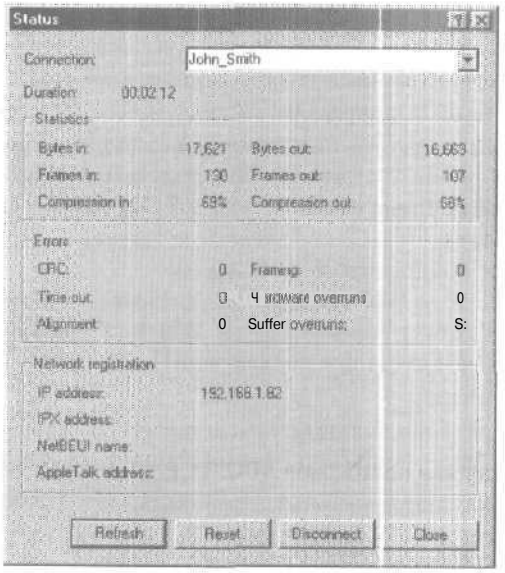


Рис. 10-13. Диалоговое окно User Status с информацией протокола TCP/IP

Для данного соединения зарегистрирован только протокол TCP/IP. Это связано с тем, что все значения группы Network Registration (Регистрация в сети), кроме IP-адреса,

не заданы. Отображаемый адрес был выделен сервером DHCP, так как сервер RAS по умолчанию использует DHCP для предоставления сетевых адресов клиентам удаленного доступа. Это можно проверить из оснастки DHCP на Server01.

Из правой панели также можно пересылать сообщения отдельным или всем подключенным клиентам удаленного доступа, а также отключать клиентов.

4. Закройте диалоговое окно Status (Состояние).
5. В меню Start (Пуск) выберите команду Run (Выполнить).
6. В поле Open (Открыть) введите **c:\winnt\system32\logfiles\iaslog.log** и щелкните кнопку OK.

   В Notepad (Блокнот) откроется журнал Accounting. Если Вы не смогли выполнить данный этап, откройте файл \Chaptl0\ex2\iaslog.log с прилагаемого компакт-диска. В данном файле лишь две записи о двух последних подключениях, установленных по учетной записи John Smith.

   Подробности об интерпретации журнала см. в справочной системе службы IAS: в поле поиска на вкладке Search (Поиск) выполните поиск фразы IAS-Formatted Log Files. Чтобы получить более читабельные файл с меньшим объемом информации, попробуйте сменить формат файла журнала на любой из форматов, совместимых с БД.
7. Закройте Notepad.
8. Чтобы просмотреть результаты регистрации событий, раскройте меню Start\ Programs\Administrative Tools (Пуск\Программы\Администрирование) и шелкните ярлык Event Viewer (Просмотр событий).

   Откроется оснастка Event Viewer, в правой панели которой отображено содержимое журнала System Log (Журнал системы).
9. Найдите и дважды щелкните событие, для которого в поле Source (Источник) указано RemoteAccess, а в поле Event ID (Событие) — 20015.

   Откроется окно свойств события удаленного доступа, показывающее подключившегося пользователя и занятый им порт.
10. Щелкните кнопку OK.
11. Найдите и дважды щелкните событие, для которого в поле Source (Источник) указано RemoteAccess, а в поле Event ID (Событие) — 20187.

    Откроется окно свойств события удаленного доступа, показывающее, что попытка аутентификации удаленного доступа была неудачна; отображается также имя пытавшегося подключиться пользователя.
12. Щелкните кнопку OK и закройте оснастку Event Viewer.

Резюме

Windows 2000 поддерживает два вида удаленного доступа: по телефонным линиям и VPN-доступ. Канал удаленного доступа по телефонным линиям включает клиент удаленного доступа, сервер удаленного доступа и инфраструктуру ГВС. Протоколы удаленного доступа управляют созданием подключений и передачей данных по ГВС-каналам. Служба RAS Windows 2000 поддерживает три протокола удаленного доступа: PPP, SLIP и Asynchronous NetBEUI. Кроме того, обеспечивается поддержка протоколов ЛВС: TCP/IP, IPX, AppleTalk и NetBEUI. Служба RAS Windows 2000 предоставляет множество возможностей зашиты, включая безопасную аутентификацию (проверку подлинности) пользователя, взаимную аутентификацию, шифрование данных, обратный вызов, номер абонента и блокировку учетной записи удаленного доступа. Управление удаленным доступом включает управление пользователями, адресами, доступом и аутентификацией.

Занятие 4. Виртуальные частные сети

Виртуальная частная сеть (virtual private network, VPN) — это расширение частной сети, содержащее инкапсулированные, зашифрованные и аутентифицированные связи внутри *разделяемых* (shared) или *общедоступных* (public) сетей. VPN обладает свойствами выделенной частной сети и позволяет передавать данные между двумя компьютерами через *межсетевое соединение* (internetwork), например Интернет. *Туннелирование*(tunneling) позволяет эмулировать соединения «точка — точка», а *виртуальные локальные сети* (virtual local area network, VLAN) — взаимодействие с ЛВС. На этом занятии дается общее представление о VPN и туннелировании, описаны настройка *сервераудаленного доступа* (remote access server, RAS) и способы устранения типичных проблем при работе с VPN.

Изучив материал этого занятия, Вы сможете:

- ✓ рассказать о характеристиках VPN и туннелирования, а также о наиболее распространенных протоколах туннелирования;
- ✓ управлять серверами VPN;
- ✓ устранять проблемы, возникающие при работе с VPN.

Продолжительность занятия — около 45 минут.

Общие сведения о VPN

Работая дома или находясь в пути, пользователи могут, применяя VPN-подключения, соединяться с сервером организации через инфраструктуру общедоступной сети (например Интернета). С точки зрения пользователя VPN-подключение выглядит как прямое соединение «точка — точка» между его компьютером (клиентом VPN) и сервером организации (сервером VPN). Конкретная инфраструктура общедоступной сети значения не имеет, так как логически данные передаются через выделенное частное подключение.

Организации могут также через VPN-подключения осуществлять маршрутизированные соединения между географически разделенными подразделениями или подключаться к серверам других организаций через общедоступные сети с поддержкой безопасной связи. Маршрутизированные VPN-подключения через Интернет логически выглядят как выделенные подключения через ГВС.

Интерфейс виртуальной сети предоставляет пользователю защищенное подключение к частной сети через общедоступную. Вместо междугороднего звонка на *сервер доступа к сети* (Network Access Server, NAS) организации пользователь может связаться с местным *поставщиком услуг Интернета* (Internet Service Provider, ISP) и по этому соединению между пользователем и VPN-сервером организации через Интернет создается виртуальная частная сеть.

Примечание Подробнее о виртуальных частных сетях см. документ \chapt10\articles\VPNoverview.doc на прилагаемом компакт-диске.

Соединение с сетью через Интернет

Для соединения с сетью организации через Интернет подразделение может использовать как выделенные, так и коммутируемые линии.

Выделенные линии

Вместо дорогих выделенных линий удаленной связи между дочерними подразделениями маршрутизаторы, установленные в них, можно подключить к местному ISP через локальную выделенную линию. VPN-подключение между маршрутизаторами выполняется через Интернет. После подключения маршрутизаторы могут отправлять пакеты друг другу по VPN.

Коммутируемые линии

Вместо междугородного звонка на сервер удаленного доступа маршрутизатор дочернего подразделения можно подключить по телефону к местному ISP. По установленному физическому соединению с местным ISP маршрутизаторы основного и дочернего подразделений связываются между собой по VPN-подключению через Интернет. Корпоративный маршрутизатор работает как сервер VPN и должен быть подключен к местному ISP через выделенную линию.

Примечание В случае выделенных и коммутируемых линий расстояние не оказывает заметного влияния на передачу данных через VPN (так как используются только локальные физические линии).

Соединение с компьютерами через интрасеть

Данные, с которыми работают некоторые отделы (например кадров), бывают столь важны, что сеть такого подразделения физически отделяют от остальной интрасети, что создает трудности для пользователей, физически не подключенных к отдельной сети.

В случае VPN-подключения сеть подразделения физически соединена с интрасетью организации, но отделена от нее сервером VPN. Последний не поддерживает прямое маршрутизированное подключение сети подразделения и интрасети организации. Пользователи интрасети, имея соответствующие права, могут установить удаленное VPN-подключение к серверу VPN и работать с защищенными ресурсами сети. Кроме того, для усиления защиты информация, передаваемая по виртуальной частной сети, шифруется. Для пользователей, не имеющих разрешений на установку VPN-подключения к сети подразделения, эта сеть недоступна (и не видна в сетевом окружении),

Основы туннелирования

Туннелирование(tunneling), или *инкапсуляция* (encapsulation), — это способ передачи информации через транзитную сеть. Такой информацией могут быть кадры (или пакеты) другого протокола. При инкапсуляции кадр не передается в сгенерированном узлом-отправителем виде, а снабжается дополнительным заголовком, содержащим информацию о маршруте, позволяющую инкапсулированным пакетам проходить через промежуточную сеть. На конце туннеля кадры деинкапсулируются и передаются получателю.

Этот процесс (включающий инкапсуляцию и передачу пакетов) и есть туннелирование. Логический путь передвижения инкапсулированных пакетов в транзитной сети называется *туннелем* (tunnel).

Обслуживание туннеля и передача данных

Протокол, сочетающий в себе функции обслуживания туннеля и передачи данных, называется *протоколом туннелирования* (tunneling protocol). Для формирования туннеля клиент и сервер туннелирования должны использовать одинаковый протокол. Такими протоколами туннелирования являются, например, PPTP и L2TP, о которых мы подробно поговорим ниже.

Протокол обслуживания туннеля

Предназначен для управления туннелем. В некоторых технологиях туннелирования, например PPTP и L2TP, туннель похож на сеанс: концы туннеля должны предварительно согласовать формирование туннеля и его параметры. Но в отличие от сеанса туннель не гарантирует надежной доставки данных. Пересылаемые по туннелю данные обычно посылаются дейтаграммным протоколом, например, UDP в случае протокола L2TP или протоколом TCP и модифицированным протоколом GRE (Generic Routing Encapsulation) в случае PPTP.

Создание туннеля

Создание туннеля инициируется клиентом туннеля путем отправки запроса на соединение другому концу туннеля — серверу туннелирования.

Процесс установления соединения при создании туннеля похож на процесс создания соединения PPP. Сервер туннелирования аутентифицирует клиента туннеля. По успешном завершении аутентификации создается туннельное соединение и данные передаются через туннель.

Клиент туннеля посылает сообщения о создании туннеля на сервер туннелирования по его межсетевому адресу. Например, при использовании Интернета клиент туннеля посылает сообщения со своего InterNIC-совместимого IP-адреса на IP-адрес сервера туннелирования. Клиент туннеля, подключенный к Интернету по коммутируемому соединению, использует в качестве исходного IP-адрес, выделенный ему местным ISP, а в качестве целевого — IP-адрес сервера туннеля.

Поддержка туннеля

В некоторых технологиях, например PPTP и L2TP, созданный туннель надо обслуживать. В частности, оба конца туннеля должны знать состояние другого конца в случае ошибки при соединении. Поддержка туннеля при отсутствии передаваемых данных обычно обеспечивается периодическими опросами одного конца туннеля другим.

Завершение работы туннеля

Для корректного завершения работы концы туннеля сообщают друг другу об окончании соединения.

Протокол передачи данных по туннелю

Инкапсулирует информацию. Клиент туннеля добавляет к данным специальный заголовок туннельного протокола передачи. Эти инкапсулированные данные и посылаются на сервер туннелирования через транзигную сеть.

Принимая пакеты, сервер туннелирования удаляет заголовок туннельного протокола и передает данные по нужному адресу. Аналогично обстоит дело и с передачей данных от сервера туннелирования клиенту туннеля.

Типы туннелей

Существует два основных типа туннелей: *заказные* (voluntary) и *принудительные* (compulsory). В зависимости от конфигурации клиента принудительные туннели могут быть *статическими* (static) и *динамическими* (dynamic).

Заказные туннели

Устанавливаются и настраиваются пользователем — клиентом туннеля. Компьютер пользователя является одним из концов туннеля и играет роль клиента.

Заказные туннели создаются, когда рабочая станция клиента запрашивает туннель у сервера туннелирования. Так как компьютер клиента берет на себя функции клиента тун-

неля, на нем должен быть установлен соответствующий протокол туннелирования. Заказные туннели применяются в одном из следующих случаев.

- Клиент уже имеет доступ к транзитной сети, способной маршрутизировать инкапсулированные данные между клиентом и сервером туннелирования.
- Наиболее распространенный вариант. Клиент должен установить удаленное подключение (по коммутируемому каналу) с транзитной сетью до настройки туннеля. Типичным пример — пользователь, имеющий доступ в Интернет по коммутируемой линии. Набрав телефон своего ISP, он получает доступ в Интернет, и может организовать туннель.

Принудительные туннели

Создаются и настраиваются автоматически. При этом функции клиента туннеля выполняет не компьютер пользователя, а другое промежуточное устройство.

Туннель может быть создан, даже если на клиентском компьютере не установлен протокол туннелирования. При этом от имени клиентского компьютера может выступать другой компьютер или сетевое устройство — *концентратор доступа* (access concentrator). Концентратор доступа должен иметь протокол туннелирования и уметь создавать туннель при подключении к нему клиентского компьютера.

При соединении через Интернет клиентский компьютер подключается к серверу сетевого доступа ISP, поддерживающему туннелирование. Например, предприятие может заключить контракт с ISP, чтобы получить в свое распоряжение сеть концентраторов доступа по всей стране. Эти концентраторы доступа могут создавать туннели с подключенным к частной сети предприятия сервером туннелирования через Интернет. Такая схема называется принудительным туннелированием, так как клиент должен использовать туннель, созданный концентратором доступа. После установления соединения весь сетевой трафик клиента (как входящий, так и исходящий) автоматически направляется по туннелю.

При принудительном туннелировании клиентский компьютер устанавливает только PPP-соединение. Когда он звонит на сервер сетевого доступа, создается туннель, по которому автоматически направляется весь трафик.

Решение о том, с каким сервером туннелирования соединить клиента, может быть принято либо на основе статической информации, хранящейся на концентраторе доступа, либо путем динамического обращения к БД пользователей.

Статические принудительные туннели

Конфигурация со статическими туннелями требует оборудования, предоставляющего доступ по выделенной линии (автоматические туннели), либо ручной настройки (туннели на основе сферы).

При автоматическом туннелировании каждому клиенту удаленного доступа назначается определенный сервер туннелирования, на который он будет автоматически направляться при соединении с концентратором доступа. Для этого нужны выделенные линии локального доступа и оборудование для сетевого доступа (это стоит недешево). Для каждого сервера туннелирования можно назначить определенный номер, набрав который, пользователь через концентратор доступа установит с ним туннель.

В схеме на базе сферы концентратор доступа принимает решение о маршруте трафика на основании части имени пользователя (сфере). Например, пользователи из сферы microsoft.com (с адресом user@microsoft.com) направляются на один сервер туннелирования, а из сферы domain.com (с адресом user@domain.com) — на другой. Туннелирование на основе сфер проще в реализации, не требует выделенных линий связи и высоких издержек после первоначальной настройки. Но внесение изменений в настройку может обойтись довольно дорого. Кроме того, трафик всех пользователей в данной сфере направляется на один конечный адрес, т. е. гибкость при выборе серверов туннелирования для разных групп пользователей здесь невелика.

Динамические принудительные туннели

Адрес назначения выбирается в момент подключения пользователя к концентратору доступа. Так как этот выбор может быть основан на самых разных параметрах (имени или адресе пользователя, номере телефона пользователя или концентратора доступа, отделе или даже времени дня), пользователи из одной сферы могут быть направлены на разные серверы туннелирования. Это делает динамическое туннелирование самым гибким методом принудительного туннелирования.

При динамическом туннелировании концентратор доступа может работать в режиме многопользовательского сервера сетевого доступа, позволяя подключаться к нему как клиентам туннеля, так и обычным клиентам Интернета — не клиентам туннеля. При этом не нужны ни выделенный концентратор доступа, ни выделенная телефонная линия. Чтобы определить, устанавливать ли туннель для позвонившего клиента, концентратор доступа опрашивает БД пользователей.

Хотя каждый концентратор дост>па может иметь собственную БД пользователей, в больших сетях это решение неэффективно из-за сложностей администрирования. Гораздо эффективнее поместить информацию о пользователях в центральное хранилище и дать концентраторам доступа при подключении клиента возможность обращаться к нему. Такое решение реализует протокол RADIUS.

Протоколы VPN

Для формирования VPN в Windows 2000 используются протоколы PPTP, L2TP, IPSEC и IP-IP. Они могут работать как вместе, так и независимо друг от друга.

PPTP

Протокол PPTP (Point-to-Point Tunneling Protocol) — расширенный протокол PPP, инкапсулирующий кадры PPP в IP-дейтаграммы для передачи их через сеть IP, например Интернет. PPTP можно использовать при соединении двух частных ЛВС.

PPTP для поддержки туннеля использует соединение TCP и передает по туннелю инкапсулированные кадры PPP, дополненные заголовками GRE. Данные в кадрах PPP могут быть зашифрованы и сжаты.-

PPTP разработан форумом PPTP, состоящим из Microsoft Corporation, Ascend Communications, 3COM, ECI Telematics и US Robotics.

Для аутентификации PPTP-туннелей используются те же механизмы, что и для аутентификации PPP-соединений, — PAP, MS-CHAP, CHAP и EAP. PPTP наследует шифрование и сжатие от PPP. В Windows 2000 шифрование PPP-кадров возможно только при использовании протокола аутентификации EAP-TLS или MS-CHAP. Шифрование PPP-кадров обеспечивает конфиденциальность только при передаче данных между концами туннеля. Обеспечить сквозную безопасную передачу позволяет протокол IPSEC. На рис. 10-14 изображен полный пакет PPTP.

Рис. 10-14, Пакет PPTP, состоящий из зашифрованных данных, заголовка и трейлера

L2TP

L2TP (Layer 2 Tunneling Protocol) является гибридом протокола PPTP и разработанной Cisco Corporation технологии Layer 2 Forwarding (L2F). Под Layer 2 здесь понимается канальный уровень.

L2TP инкапсулирует кадры PPP и передает их по сетям IP, X.25, Frame Relay или ATM. Инкапсулируя свои дейтаграммы в IP-пакеты, L2TP действует как протокол туннелирования через Интернет. L2TP можно также использовать при соединении двух частных ЛВС.

L2TP также использует протокол UDP для передачи по туннелю инкапсулированных кадров PPP. Полезные данные инкапсулированных кадров PPP могут быть зашифрованы и сжаты, В Microsoft в качестве метода шифрования для L2TP выбран IPSec, а не PPP. И все же другие реализации L2TP могут использовать шифрование PPP. На рис. 10-15 изображен пакет L2TP, подготовленный для передачи через соединение «точка — точка» в ГВС (например, по телефонной линии) и использующий параметры IPSec для аутентификации и шифрования. Здесь также показаны этапы обработки пакета. Этапы 1–4 соответствуют обычной обработке, предшествующей инкапсуляции по IPSec. Инкапсуляция производится на этапах 5–7. На остальных этапах осуществляется доставка пакета по адресу назначения.

Примечание В Windows 2000 протокол L2TP работает только в сети IP. Его нельзя использовать при работе в основном режиме в сетях X.25, Frame Relay или ATM.

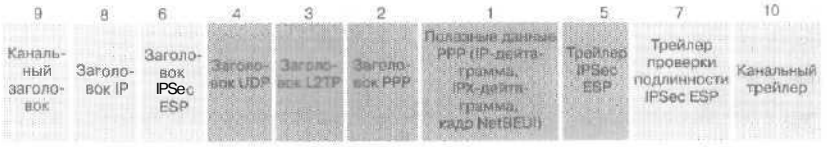


Рис. 10-15. Пакет L2TP с зашифрованными данными и дополнительными заголовками

L2TP действует приблизительно так же, как и PPTP. Между клиентом и сервером L2TP создается L2TP-туннель. Для доступа к серверу туннелирования через межсетевое соединение IP-клиент может использовать либо ЛВС. либо удаленное соединение с сервером доступа к сети.

Для аутентификации туннелей L2TP используются те же механизмы, что и для аутентификации соединений PPP: PAP, MS-CHAP, CHAP и EAP. L2TP наследует от протокола PPP сжатие, но не шифрование. Шифрование PPP не используется из-за несоответствия требованиям безопасности, предъявляемым L2TP. Дело в том, что шифрование PPP, хоть и гарантирует конфиденциальность, не обеспечивает аутентификацию, целостность и защиту от повторов для каждого пакета. Поэтому данные шифруются по технологии IPSec. А использовать шифрование соединения PPP, когда данные уже зашифрованы с помощью IPSec, нет смысла, так как это приведет к дополнительным затратам на обработку данных и не даст существенной выгоды.

Сравнительная характеристика протоколов PPTP и L2TP

Как PPTP, так и L2TP используют PPP для установления соединений «точка — точка» в ГВС, формируя с его помощью исходные данные и дополняя их заголовками. Однако между PPTP и L2TP есть и различия:

- PPTP работает только в сетях IP, тогда как L2TP поддерживает любую пакетно-ориентированную среду передачи данных по туннелю, где возможна организация одноранговых подключений; в частности, L2TP может функционировать в сетях IP (с помощью UDP), частных виртуальных каналах (PVC) Frame Relay, X.25 VC и ATM VC;
- L2TP поддерживает сжатие заголовков, при этом заголовок дополняется 4 байтами, тогда как в случае PPTP — 6;
- L2TP в отличие от PPTP поддерживает аутентификацию туннеля; впрочем, при использовании IPSec аутентификация туннеля обеспечивается автоматически, и необходимость в ней для L2TP отпадает;
- PPTP использует шифрование на основе PPP, а Microsoft-реализация L2TP требует для шифрования IPSec.

IPSec

IPSec — туннельный протокол 3-го уровня — представляет собой набор стандартов, поддерживающих безопасную передачу через транзитную IP-сеть. Режим туннеля *с* безопасной *инкапсуляцией полезных данных* (Encapsulating Security Payload, ESP) поддерживает инкапсуляцию и шифрование IP-дейтаграмм, обеспечивая их безопасную передачу через частную или общедоступную IP-сеть

При работе IPSec в туннельном режиме ESP дейтаграмма IP полностью инкапсулируется и шифруется с помощью ESP. Полученный результат снова инкапсулируется (используя нешифрованный заголовок IP) и посылается через транзитную сеть (рис. 10-15).

Получив зашифрованную дейтаграмму, сервер туннеля обрабатывает и удаляет заголовок IP, а затем аутентифицирует и расшифровывает ESP- и IP-пакет. После этого происходит обычная обработка IP-пакета, включая доставку пакета адресату.

Транспортный режим ESP

В пакет инкапсулируется заголовок IP, позволяющий доставить пакет до конечного адреса после его выхода из туннеля (т. е. после удаления инкапсуляции и шифрования IPSec). В транспортном режиме ESP пакет всегда дешифруется только по достижении адресата.

Структура пакета IPSec в режиме туннеля

Существует несколько уровней инкапсуляции пакета IPSec в режиме туннеля (рис. 10-15):

- первый уровень: к исходной IP-дейтаграмме добавляется трейлер ESP, после чего происходит шифрование (шаг 5 на рис. 10-15);
- второй уровень: зашифрованные данные инкапсулируются — к ним добавляется заголовок ESP и трейлер проверки подлинности ESP; последний содержит *значение проверки целостности* (Integrity Check Value, ICV) — криптографическую контрольную сумму для проверки подлинности и целостности передаваемой информации (шаги 6 и 7);
- третий уровень: к пакету IPSec добавляется заголовок IP, содержащий информацию об IP-адресах концов туннеля (шаг 8);
- канальный уровень: чтобы IP-дейтаграмма могла быть отправлена по ЛВС или ГВС, к ней приписываются заголовок и трейлер канального уровня, обрабатываемые на канальном уровне исходящего физического интерфейса (шаги 9 и 10).

Режим туннеля протокола IPSec соответствует сетевому уровню модели OSI- В отличие от L2TP и PPTP он не использует PPP для обеспечения безопасности и аутентификации. Кроме того, его нельзя задействовать в качестве интерфейса маршрутизатора Windows 2000 (в отличие от IP-IP), поэтому он не поддерживает маршрутизируемые протоколы и коммутируемые соединения по запросу. Вместо этого режим туннеля IPSec можно задей-

ствовать на основе фильтров пакетов для каждого маршрута, которые позволяют определить адресата туннеля IPSec.

IP-IP

IP-IP (или «IP в IP») — простая технология туннелирования, соответствующая третьему уровню модели OSI (сетевой уровень). Виртуальная сеть создается путем инкапсуляции IP-пакета с помощью дополнительного заголовка IP. Главное назначение IP-IP — туннелирование многоадресного трафика в частях сети, не поддерживающих многоадресную маршрутизацию. Структура пакета IP-IP состоит из внешнего IP-заголовка, туннельного заголовка, внутреннего IP-заголовка и полезных IP-данных.

Данные IP включают в себя информацию, получаемую от верхних уровней: заголовки TCP, UDP или ICMP, а также исходные данные. Стандартные сообщения ICMP предлагают некоторые ограниченные возможности по поддержке туннеля, позволяя туннелю определять значение *максимальной единицы передачи данных* (Maximum Transfer Unit, MTU), обнаруживать перегрузку сети и ошибки маршрутизации.

Управление виртуальными частными сетями

На занятии 3 Вы узнали об управлении удаленным доступом. Управление VPN во многом на него похоже. Оно должно подчиняться тем же принципам, что и управление другими сетевыми ресурсами. В частности, особое внимание надо уделить безопасности, особенно если VPN организована через Интернет.

Управление пользователями

Так как размещать учетные записи одного пользователя на разных серверах непрактично, большинство администраторов создают главную БД учетных записей на контроллере домена или сервере RADIUS. Это позволяет серверу VPN отправлять сведения об аутентификации на центральное устройство аутентификации. Для удаленного доступа через коммутируемое или VPN-подключение применяются одни и те же учетные записи.

Управление адресами и серверами имен

Сервер VPN должен иметь свободные IP-адреса для назначения виртуальному интерфейсу VPN-сервера и VPN-клиентам в ходе согласования параметров подключения IPCP (IP Control Protocol). Назначаемый VPN-клиенту IP-адрес присваивается его виртуальному интерфейсу.

Сервер VPN на основе Windows 2000 по умолчанию получает IP-адреса, назначаемые VPN-клиентам, через DHCP. Можно также сконфигурировать статический пул IP-адресов. Кроме того, при настройке сервера VPN надо указать адреса серверов разрешения имен (серверов DNS и WINS), назначаемых VPN-клиенту в ходе IPCP-согласования.

Управление доступом

В Windows 2000 для управления коммутируемыми сетевыми и VPN-подключениями можно задавать параметры удаленного доступа для отдельных учетных записей пользователей, а также политики удаленного доступа.

Доступ по учетной записи пользователя

Для настройки разрешений удаленного доступа отдельного пользователя служит вкладка Dial-In диалогового окна свойств учетной записи пользователя. Чтобы разрешить пользователю устанавливать подключения VPN, выберите переключатель Allow Access. Если с

сервером VPN могут устанавливаться только VPN-подключения, удалите действующую по умолчанию политику удаленного доступа Allow Access If Dial-In Permission Is Enabled. Затем создайте новую политику удаленного доступа, дав ей содержательное имя.

Внимание! После того как политика удаленного доступа, заданная по умолчанию, была удалена, клиенту, не удовлетворяющему хотя бы одному условию в созданной Вами политике, будет отказано в удаленном доступе.

Если к серверу VPN можно осуществить удаленный доступ по коммутируемому соединению, не удаляйте стандартную политику удаленного доступа — переместите ее, чтобы она применялась к клиенту в последнюю очередь.

Управление доступом посредством групп

Если Вы хотите управлять удаленным доступом на основе групп, выберите переключатель Control Access Through Remote Access Policy (Управление на основе политики удаленного доступа) для всех учетных записей. Создайте труппу Windows 2000, включив в нее пользователей, которым разрешено создавать VPN-соединения. Если с сервером VPN могут устанавливаться только VPN-соединения, удалите действующую по умолчанию политику удаленного доступа Allow Access If Dial-In Permission Is Enabled. Затем создайте новую политику удаленного доступа, дав ей содержательное имя, и назначьте ее для этой группы.

Если к серверу VPN можно осуществить удаленный доступ по коммутируемому соединению, не удаляйте стандартную политику удаленного доступа — переместите ее, чтобы она применялась к клиенту в последнюю очередь.

Управление аутентификацией

В качестве поставщика служб проверки подлинности для сервера VPN можно выбрать как Windows, так и RADIUS. В первом случае пользователи, пытающиеся установить VPN-соединение, аутентифицируются средствами Windows и политики удаленного доступа, настраиваемой из оснастки Routing And Remote Access.

Во втором случае реквизиты пользователей и параметры запрашиваемого подключения направляются на сервер RADIUS.

Получив сообщение о запросе пользователя на подключение к серверу VPN, сервер RADIUS проверяет пользователя по своей БД аутентификации. В центральной БД сервера RADIUS могут храниться параметры пользователя, поэтому, кроме положительного или отрицательного ответа на запрос об аутентификации, сервер RADIUS может сообщать серверу VPN и другие параметры подключения, например максимальное время сеанса, выделяемые пользователям статические IP-адреса и др. Сервер IAS RADIUS хранит сведения о профиле удаленного доступа для клиентов, использующих сервер RADIUS в качестве поставщика проверки подлинности. Если сервер RAS использует аутентификацию RADIUS, то в дереве консоли оснастки Routing And Remote Access не отображается узел Remote Access Policies. При этом для настройки политики удаленного доступа надо использовать IAS.

Для ответов на запросы об аутентификации RADIUS может использовать или другой сервер БД, например ODBC-источник, или контроллер домена Windows 2000. Последний может располагаться как на том же компьютере, что и сервер RADIUS, так и в другом месте. Кроме того, сервер RADIUS может играть роль прокси-клиента для удаленного сервера RADIUS.

Устранение неполадок

При работе с VPN могут возникать проблемы, связанные с IP-соединениями, установлением подключений удаленного доступа, маршрутизацией и IPSec:

- отказ в доступе, тогда как он должен быть разрешен;
- разрешение доступа, тогда как в нем должно быть отказано;
- ошибка доступа к ресурсам за пределами VPN-сервера;
- ошибка формирования туннеля.

Отказ в доступе, тогда как он должен быть разрешен

Для решения этой проблемы попробуйте сделать следующее.

- Проверьте, можно ли обратиться к серверу VPN с помощью утилиты ping (задав имя хоста или IP-адрес сервера VPN). Если задано имя хоста, убедитесь, что оно разрешается в правильный IP-адрес.
- Проверьте, запущена ли на сервере VPN служба RRAS.
- Проверьте, есть ли свободные порты PPTP или L2TP на сервере VPN. При необходимости измените число этих портов, увеличив максимальное число параллельных подключений, из узла Ports (Порты) оснастки Routing And Remote Access.
- Убедитесь, что используемый клиентом VPN протокол туннелирования поддерживается сервером VPN, проверив свойства портов на сервере RAS.
- Для клиентов удаленного доступа VPN по умолчанию тип сервера выбирается автоматически, т. е. сначала они пытаются установить туннель PPTP, а затем L2TP поверх IPSec. Если же в качестве типа сервера выбран PPTP или L2TP, проверьте, поддерживается ли сервером VPN соответствующий протокол туннелирования.
- Windows 2000-компьютер, на котором запущена RRAS, является сервером PPTP и L2TP и по умолчанию имеет по пять PPTP- и L2TP-портов; количество портов можно увидеть в левой панели узла Ports оснастки Routing And Remote Access; чтобы компьютер выполнял функции только сервера PPTP, удалите порты L2TP.

  Чтобы компьютер был только сервером L2TP, задайте количество портов PPTP равным 1 (так как число портов PPTP не может быть равно 0), а затем в узле Ports (Порты) сбросьте флажки Remote Access Connection (Inbound Only) и Demand Dial Routing Connections (Inbound And Outbound); на клиентском компьютере измените тип сервера VPN с автоматического на L2TP.
- Убедитесь, что клиент и сервер VPN применяют хотя бы один общий метод аутентификации.
- Если используется соединение PPTP, проверьте, можно ли его установить без шифрования. Если да, проверьте параметры шифрования на клиенте и сервере VPN.
- Если используется соединение L2TP поверх IPSec, проверьте, может ли оно быть установлено без шифрования (без IPSec). Если да, проверьте параметры шифрования L2TP поверх IPSec на клиенте и сервере VPN.

  Чтобы отключить IPSec на клиентском компьютере, в окне свойств VPN-соединения перейдите на вкладку Networking и откройте окно свойств TCP/IP. Щелкнув кнопку Advanced, перейдите на вкладку Options. Откройте диалоговое окно IP Security и укажите в нем, что клиент не должен использовать IPSec.

  Чтобы отключить IPSec на сервере, из окна свойств локальной сетевой платы перейдите к свойствам TCP/IP, а затем проделайте шаги, аналогичные описанным для клиента. С сервера эту процедуру можно затем выполнить и для клиентского компьютера,

если у последнего в окне Network And Dial-up Connections (Сеть и удаленный доступ к сети) имеется значок Local Area Connection (Подключение по локальной сети).

- Проверьте, установлены ли политиками удаленного доступа разрешения для параметров подключения. Установка политик удаленного доступа производится из оснастки Routing And Remote Access или на сервере RADIUS (в зависимости от поставщика проверки подлинности).

Чтобы подключение могло быть установлено, его параметры должны:

- соответствовать всем условиям хотя бы одной политики удаленного доступа;
- иметь разрешение на удаленный доступ; это разрешение можно задать в объекте пользователя или через комбинацию параметров объекта пользователя и политик удаленного доступа; в последнем случае для этого надо в окне свойств объекта пользователя выбрать параметр Control Access Through Remote Access Policy, а в окне свойств групповой политики — Grant Remote Access Permission;
- соответствовать всем параметрам профиля;
- соответствовать всем параметрам удаленного доступа объекта пользователя. при этом параметры профиля политики удаленного доступа не должны противоречить параметрам маршрутизации и сервера удаленного доступа.

Если параметры профиля политики противоречат параметрам сервера VPN, попытка соединения будет отклонена. Например, если в политике удаленного доступа указано, что для аутентификации надо использовать протокол EAP-TLS, а сервер VPN его не поддерживает, соединение с сервером VPN установлено не будет,

- Убедитесь, что сведения о клиенте VPN (имя пользователя, пароль, имя домена) правильны и могут быть опознаны сервером VPN.
- Если сервер VPN использует статический пул IP-адресов, проверьте, хватает ли адресов в пуле. Если все адреса пула уже выделены установившим соединение VPN-клиентам, сервер VPN не сможет выделить IP-адрес новому клиенту и попытка подключения будет отклонена.
- Проверьте конфигурацию поставщика проверки подлинности. Если сервер VPN — член домена Windows 2000 в основном или смешанном режиме использует аутентификацию Windows NT, убедитесь, что учетная запись компьютера с сервером VPN включена в группы безопасности серверов RAS и IAS.
- Проверьте, поддерживает ли VPN-сервер подключения удаленного доступа (если устанавливаемое VPN-подключение является подключением удаленного доступа).
- Проверьте, поддерживают ли порты PPTP и/или L2TP входящие запросы на удаленный доступ (если устанавливаемое VPN-подключение является подключением удаленного доступа).
- Убедитесь, что применяемые VPN-клиентом протоколы ЛВС поддерживают удаленный доступ (если VPN-клиент — удаленный).
- Для VPN-подключений типа «маршрутизатор — маршрутизатор» убедитесь, что маршрутизация включена и для сервера VPN выбрана маршрутизация в ЛВС и по требованию. Этот параметр можно задать на вкладке General (Общие) диалогового окна свойств сервера RRAS.
- Для соединений VPN типа «маршрутизатор — маршрутизатор» убедитесь, что порты PPTP и L2TP поддерживают входящие и исходящие соединения маршрутизации по требованию. Этот параметр можно задать в окне свойств узла Ports.

Доступ разрешен, тогда как в нем должно быть отказано

Прежде всего убедитесь, что это не следствие применения политик удаленного доступа. Попытка подключения отклоняется, если:

- для объекта пользователя запрещен удаленный доступ;
- для объекта пользователя задано разрешение удаленного доступаControl Access Through Remote Access Policy и для первой политики, удовлетворяющей параметрам запрашиваемого подключения, выбран параметр Deny Remote Access Permission.

Ошибка при доступе к ресурсам за пределами сервера VPN

Чтобы решить эту проблему, выполните следующие действия.

- Удостоверьтесь, что для протоколов ЛВС, используемых клиентамиVPN, выбран параметр Entire network.
- Проверьте пул IP-адресов сервераVPN.
  - Если VPN-сервер настроен на использование статического пулаадресов, проверьте, что маршруты к диапазонам адресов, заданным в нем, доступны для компьютеров и маршрутизаторов интрасети. Если это не так, на маршрутизаторах интранет надо добавить IP-маршруты, состоящие из диапазонов адресов из статического пула, указав IP-адрес и маску для каждого диапазона. Либо включите протокол маршрутизации на VPN-сервере, соответствующий инфраструктуре сети. Если маршруты к подсетям VPN-клиентов удаленного доступа отсутствуют, эти клиенты не могут получать пакеты из интрасети. Маршруты для сети определяются через статические записи о маршрутах или по протоколу маршрутизации (например OSPF или RIP).
  - Если VPN-сервер настроен на протокол DHCP для назначения IP-адресов, но DHCP-сервер недоступен, VPN-сервер использует адреса из диапазона APIPA (Automatic Private IP Addressing) с 169.254.0.1 по 169,254.255.254. Выделение APIPA-адресов для удаленных клиентов возможно, только если в сети, к которой подключен VPN-сервер, тоже используются APIPA-адреса.
  - Если статический пул состоит из диапазонов IP-адресов, являющихся подмножеством диапазона IP-адресов, используемого в сети, к которой подключен VPN-сервер, проверьте, что эти диапазоны не назначены другим узлам TCP/IP (через статическую конфигурацию или с помощью DHCP).
  - Для соединения VPN типа «маршрутизатор — маршрутизатор» убедитесь, что оно интерпретируется сервером VPN корректно (а не как соединение удаленного доступа).
  - Если в диспетчере Routing And Remote Access Manager в списке Dial-In Clients для запрашивающего соединение маршрутизатора отображается имя пользователя, значит, сервер VPN интерпретирует маршрутизатор в качестве клиента удаленного доступа. При этом проверьте, совпадает ли имя пользователя для маршрутизатора с именем интерфейса маршрутизации по требованию на сервере VPN.

Ошибка при установлении туннеля

Чтобы решить эту проблему, выполните следующие действия.

- Проверьте правильность адреса. Старайтесь использовать IP-адрес ближайшего к Вам интерфейса сервера, т. е. интерфейса, который обладает обратным маршрутом. При разрешении IP-адресов с помощью DNS может применяться неправильный адрес, что приведет к сбросу сеанса PPTP.

- Убедитесь, что фильтрация пакетов, осуществляемая интерфейсом маршрутизатора между клиентом и сервером VPN, не препятствует передаче данных по туннелю:
  - на сервере VPN с Windows 2000 настройка фильтрации IP-пакетов производится из окна дополнительных свойств TCP/IP и из оснастки Routing And Remote Access; примените оба инструмента, чтобы определить, не ограничивают ли фильтры трафик VPN;
  - убедитесь, что фильтрация пакетов на других маршрутизаторах не блокирует нужные протоколы;
  - проверьте, что конфигурация протоколов туннелирования следующая:
    - PPTP: порт TCP — 1723, ID протокола IP для сеанса управления и GRE — 47;
    - L2TP: порт UDP - 1701;
    - IPSec: ID протокола для заголовка проверки подлинности IPSEC и ESP— 50 и 51;
    - **IP-IP: ID** протокола IP — 4.
- Убедитесь, что на клиенте VPN не запущен прокси-клиент WmSock. Если это так, то вызовы WmSock API (в частности те, что применяются для создания туннеля и отправки данных по туннелю) перехватываются и передаются сконфигурированному для этого прокси-серверу.

Резюме

VPN обладает свойствами выделенной частной сети, поддерживая передачу данных между двумя компьютерами через транзитную сеть, например Интернет. Для соединения с сетью организации через Интернет подразделение организации может использовать как выделенные, так и коммутируемые линии. VPN передает информацию с помощью туннелирования — метода передачи через транзитную сеть. Протокол туннелирования состоит из протокола поддержки туннеля и протокола передачи данных через туннель. Существует два основных типа туннелей — заказные и принудительные. Для соединений VPN в Windows 2000 используются протоколы PPTP, L2TP, IPSec и IP-IP. Управление VPN включает в себя управление пользователями, адресами и серверами имен, доступом, аутентификацией и шифрованием. Проблемы, возникающие при работе с VPN, могут быть связаны с IP-соединениями, установлением подключений удаленного доступа, маршрутизацией и IPSec-

Занятие 5. Средства управления службой RRAS

В Windows 2000 включены средства управления RRAS и устранения неполадок: оснастка Routing And Remote Access, утилита командной строки netsh, протоколирование аутентификации, учета, событий, а также трассировка.

Изучив материал этого занятия, Вы сможете:

✓ средствами Windows 2000 управлять RRAS и устранять неполадки,

Продолжительность занятия — около 30 минут.

Оснастка Routing And Remote Access

Позволяет выполнять ряд функций управления, таких как активизация RRAS, управление интерфейсом маршрутизации, конфигурирование политики удаленного доступа и т. д. Для получения дополнительной информации о Routing And Remote Access откройте ее и щелкните кнопку Help (рис. 10-16).

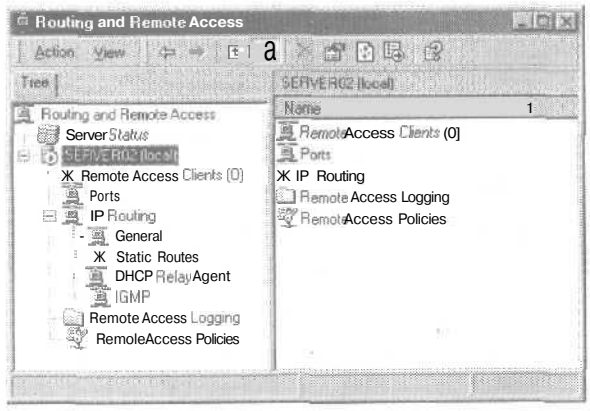


Рис. 10-16. Оснастка Routing And Remote Access (Маршрутизация и удаленный доступ)

Ярлык оснастки находится в программной группе Administrative Tools (Администрирование). Routing And Remote Access — основная утилита конфигурирования локальных и удаленных серверов и маршрутизаторов Windows 2000.

Утилита командной строки Net Shell

Служит для написания сценариев настройки и контроля сетевых компонентов Windows 2000. Утилита Net Shell называется Netsh.exe и во время установки Windows 2000 размещается в папке %systemroot%\ system32. Netsh позволяет также сохранять сценарий конфигурации в текстовом файле для архивных целей или для конфигурирования других серверов,

Netsh может поддерживать компоненты Windows 2000, добавляя вспомогательные DLL-файлы. Они расширяют функциональность netsh, предоставляя дополнительные команды для просмотра или конфигурирования сетевого компонента Windows 2000. Например, Ippromon.dll — вспомогательный файл для использования команд dhcp, dnsproxy, igmp, nat, ospf, dhcp relay и rip. Каждый вспомогательный DLL-файл имеет свой контекст - набор команд для настройки сетевого компонента. Внутри каждого контекста могут нахо-

диться подчиненные контексты. Например, внутри контекста маршрутизации находятся подчиненные контексты ip и ipx для группировки команд маршрутизаторов IP и IPX.

Примечание Параметры командной строки, начинающиеся со знака минуса (–), выполняются вне режима Shell. В режиме Shell команды выполняются без указания netsh или команды, начинающейся со знака (–).

Параметры командной строки netsh таковы.

- **–a** <*файл-псевдоним*> указывает, что может быть использован файл псевдонима. Последний содержит список команд netsh и версию псевдонима, так что командная строка псевдонима может быть использована вместо команды netsh. Файл псевдонима может быть использован для привязки команд к команде netsh, которая может быть более известна в других платформах.
- **–a** <*контекст*> указывает контекст команды в соответствии с установленным вспомогательным DLL-фалом. Например:

  ```
  netsh -c routing
  ```

  переводит Вас в контекст маршрутизатора.
- команда указывает, какую команду netsh выполнять. Команды могут выполняться как внутри, так и вне оболочки. Например:

  ```
  netsh show helper
  ```

  показывает вспомогательные файлы, установленные в корне оболочки. После входа в оболочку (для входа набрать netsh) команда для показа вспомогательных DLL-файлов в корне netsh выглядит так:

  ```
  show helper
  ```
- **–f** <*файл_сценария*> указывает, что надо выполнить все команды netsh из файла сценария. Например:

  ```
  netsh -f config.txt
  ```

  выполняет все команды из файла config.txt.
- -r<*имя_удаленного_компьютераили IP-адрес*> указывает, что команды netsh выполняются на удаленном компьютере с соответствующим именем или IP-адресом. Например:

  ```
  netsh -r RRAS2
  ```

  инициирует выполнение команд Net Shell для сервера удаленного доступа с именем RRAS2.

  Командная строка принимает вид:

  ```
  [RRAS2] netsh>
  ```

Команды разрешается сокращать до кратчайшего уникального эквивалента. Например, ro ip sh int в оболочке соответствует routing ip show interface. Команды netsh могут быть глобальными или контекстными. Первые выполняются в любом контексте и отвечают за базовые функции netsh, вторые меняются в соответствии с контекстом.

Глобальные команда netsh таковы:

Команда	Описание
..	Подъем на один контекстный уровень вверх.
? или help	Вывод справки.
add helper	Добавление вспомогательного DLL-файла.
delete helper	Удаление вспомогательного DLL-файла.
show helper	Вывод списка установленных вспомогательных DLL-файлов.
online	Установка интерактивного режима работы. Любые изменения, выполненные в этом режиме, немедленно отражаются в маршрутизаторе.
offline	Установка автономного режима работы. Все изменения, сделанные в этом режиме, будут сохранены, но для их установки в маршрутизаторе требуется команда commit или online.
set mode	Установка интерактивного или автономного режима работы.
show mode	Отображает текущий режим.
flush	Отмена любых изменений, сделанных в автономном режиме.
commit	Вносит изменения, сделанные в автономном режиме.
set machine	Конфигурирует компьютер, на котором выполняются команды netsh.
show machine	Отображает компьютер, на котором выполняются команды netsh.
exec	Выполняет файл сценария с командами netsh.
quit или bye или exit	Выход из netsh.
add alias	Добавляет псевдоним к существующей команде.
delete alias	Удаляет псевдоним из существующей команды.
show alias	Отображает все определенные псевдонимы.
dump	Сохранение копии конфигурации в текстовом файле.
popd	Извлечение контекста из стека.
pushd	Помещение текущего контекста в стек.

Netsh имеет следующие командные режимы.

- **Интерактивный** — команды, вводимые в командной строке netsh, выполняются немедленно.
- **Автономный** — команды, вводимые в командной строке netsh, накапливаются и выполняются в виде пакета после ввода глобальной команды commit. Накопленные команды могут быть отменены глобальной командой flush.

Вы можете также выполнить сценарий (текстовый файл, содержащий список команд netsh), используя параметр командной строки –f или введя глобальную команду exec в оболочке netsh.

Для создания сценария текущей конфигурации служит глобальная команда dump. Эта команда генерирует выполняющуюся в данный момент конфигурацию в виде команд netsh. Потом Вы можете использовать созданный этой командой сценарий для конфигурирования нового сервера или изменения конфигурации имеющегося. Если Вы вносите дополнительные изменения в конфигурацию компонента, рекомендуется начать сеанс конфигурирования с команды dump, на случай восстановления исходной конфигурации.

Для RRAS команда netsh имеет контексты:

- ras — команды для конфигурирования удаленного доступа;
- **aaaa** — команды для конфигурирования компонента AAAA, используемого службами маршрутизации и удаленного доступа и проверки подлинности в Интернете; AAAA хранит настройку конфигурации сервера IAS;
- **routing** — команды для конфигурирования маршрутов IP и IPX;
- **interface** — команды для конфигурирования интерфейса вызова по требованию.

О командах разных контекстов см. также справочную систему Windows 2000 Server и справку команды netsh.

Протоколирование аутентификации и учета

RRAS поддерживает протоколирование аутентификации и учетной информации для попыток подключения на основе PPP, когда проверка подлинности выполняется средствами Windows 2000. Журнал PPP-соединений отделен от системного журнала. Записанная информация позволяет Вам отслеживать использование удаленного доступа и попыток аутентификации. Протоколирование аутентификации особенно полезно при устранении ошибок политики удаленного доступа. Для каждой попытки аутентификации записывается наименование политики удаленного доступа, которая либо приняла, либо отвергла попытку подключения.

Аутентификация и учетная информация хранятся в конфигурируемом журнале или в файлах в папке %systemroot%\System32\LogFiles. Журналы сохраняются в формате IAS 1.0 или в формате БД, т. е. любая программа СУБД может напрямую считывать журнал для анализа.

Вы можете настроить тип регистрируемых операций (учет или аутентификация) и параметры журнала, включая альтернативное место хранения, через свойства папки Remote Access Logging либо в оснастке Routing And Remote Access, либо в оснастке Internet Authentication Service (Служба проверки подлинности в Интеренете). Расположение журнала зависит от параметров поставщика служб проверки подлинности, используемого RRAS.

Регистрация событий

Маршрутизатор Windows 2000 выполняет расширенное протоколирование ошибок в системном журнале. Информацию журналов событий можно использовать для устранения ошибок маршрутизации или процессов удаленного доступа.

Существуют четыре уровня протоколирования:

- только ошибки;
- ошибки и предупреждения;
- максимальное количество информации;
- отключить протоколирование событий.

Так, если маршрутизатор Open Shortest Path First (OSPF) не может установить привязку к интерфейсу, можно:

1. отключить OSPF на интерфейсе;
2. изменить уровень регистрации для OSPF, чтобы записывалось максимальное количество информации;
3. включить OSPF для интерфейса;
4. изучить действия процесса OSPF к журнале системных событий;
5. изменить уровень регистрации, чтобы записывались только ошибки.

Затем можно устранить проблему привязки, анализируя записи OSPF в журнале системных событий.

Уровень регистрации событий можно настроить из разных мест оснастки Routing And Remote Access. Например, для определенного компьютера протоколирование можно установить на вкладке Event Logging свойств компьютера, Можно также включить протоколирование в диалоговом окне свойств IP Routing.

Трассировка

Маршрутизатор Windows 2000 обладает богатыми возможностями трассировки, полезными для устранения сложных сетевых неполадок. Компоненты Windows 2000 Server могут записывать трассировочную информацию в файлы. Чтобы включить трассировку, нужно изменить параметры реестра Windows 2000 в разделе:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing
```

Внимание! Без крайней необходимости не используйте редактор реестра. Редакторы реестра обходят стандартные средства защиты, предоставляемые административными утилитами. Эти средства зашиты предохраняют Вас от ввода конфликтных параметров или параметров, способных снизить эффективность или повредить систему. Прямое редактирование реестра может иметь серьезные и неожиданные последствия, способные сделать загрузку системы невозможной и вызвать необходимость переустановки Windows 2000. При возможности для конфигурирования Windows 2000 используйте программы из панели управления или оснастки.

Трассировка включается для каждого протокола маршрутизации отдельно параметрами реестра, описанными ниже. Трассировку для протоколов маршрутизации можно включать/отключать в процессе работы маршрутизатора. Каждый протокол маршрутизации обладает возможностями трассировки и имеет соответствующий подраздел (например OSPF или RIPV2) в приведенном выше разделе реестра.

Трассировка занимает системные ресурсы, и ее следует применять только для выявления сетевых неполадок. Получив данные или выявив причины неполадки, сразу же отключите трассировку. Не оставляйте ее включенной на компьютерах с несколькими процессорами.

Трассировочная информация может быть сложной и очень подробной. **Большая** ее часть полезна только инженерам службы поддержки Microsoft или сетевым администраторам, имеющим большой опыт работы с маршрутизатором Windows 2000.

Трассировка в файл

Чтобы включить трассировку для каждого протокола маршрутизации, задайте следующим параметрам в соответствующих подразделах реестра такие значения:

- EnabJeFileTracing REG_DWORD 1

  Чтобы включить запись трассировочной информации в файл, присвойте этому параметру значение 1; значение по умолчанию — 0.

- FileDirectory REG_EXPAND_SZ *путь*

  Чтобы изменить местоположение по умолчанию для файлов трассировки, задайте новый путь в параметре I ileDirectory. Именем фай ia трассировки служит имя компонента, для которого выполняется трассировка. По умолчанию файлы трассировки находятся в папке %systemroot%\Tracing.

- FileTracingMask REG_DWORD *ОбъемРегистрируемойТрассировочнойИнформации*
  Параметр FileTracingMask определяет степень подробности записываемой в файл трассировочной информации; значение по умолчанию — FFFF0000.
- MaxFileSize REG_DWORD *РазмерФайлаЖурнала*
  Параметр MaxFileSize позволяет задать размер файла журнала. Значение по умолчанию - 10000 (64кб).

Резюме

Оснастка Routing And Remote Access позволяет выполнять множество задач, например включение RRAS, управление интерфейсом маршрутизации, конфигурирование IPX-маршрутизации, создание пула статических IP-адресов, конфигурирование политик удаленного доступа и т. д. Netsh — это утилита командной строки для настройки сетевых компонентов Windows 2000 локальных и удаленных компьютеров, поддерживающая сценарии. RRAS также поддерживает регистрацию аутентификации и учетной информации для попыток связи на основе PPP, если аутентификация выполняется средствами Windows. Кроме того, маршрутизатор Windows 2000 выполняет дополнительную регистрацию ошибок в системном журнале. Вы можете использовать информацию в журналах событий для устранения ошибок маршрутизации или процессов удаленного доступа. Windows 2000 способна также выполнять дополнительную трассировку работы RRAS, для устранения сложных сетевых ошибок

Закрепление материала

? J Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Поясните назначение маршрутизации вызова по требованию.

2. Какие поставщики служб проверки подлинности существуют в RRAS и чем они отличаются от методов аутентификации?

3. Каково назначение VPN и какие две технологии VPN поддерживает RRAS в Windows 2000?

4. Клиент удаленного доступа начинает подключаться к серверу RRAS, но соединение прерывается. Как устранить эту ошибку?

5. В чем сходство разрешения удаленного доступа Deny Access (Запретить доступ) (в смешанном или основном режиме) с политикой удаленного доступа по умолчанию в домене основного режима?

6. Вам надо сконфигурировать 10 серверов RRAS для клиента. Все будут иметь одинаковые конфигурации RRAS. Как наиболее эффективно выполнить эту задачу?

ГЛАВА 11

Система безопасности Windows 2000

В этой главе

В Microsoft Windows 2000 реализована полная *инфраструктура открытого шифрувального ключа* (public key infrastructure, PKI). PKI расширяет возможности криптографических служб *открытого ключа* (public key, PK) для Windows, поставлявшихся в последние годы, предоставляя интегрированный набор служб и средств администрирования для создания, распространения и управления PK-приложениями. Здесь рассматривается Windows 2000 PKI, обсуждаются основные технологии открытого ключа, поддерживаемые Windows 2000, и дан краткий обзор протоколов Kerberos и IPSec. Вы познакомитесь со встроенными средствами конфигурации защиты и системой аудита, обеспечивающей безопасность сети.

Примечание Система безопасности Windows 2000 — это эффективный и всеохватывающий набор служб. Хотя эта глава призвана познакомить Вас со средствами защиты Windows 2000, подробно рассмотреть все аспекты мы не сможем. Рекомендуем Вам изучить соответствующие материалы в справочной системе Windows 2000 и на узле Microsoft в Интернете (*http://wwwmicrosoft.com*).Кроме того, в данный курс включены важные статьи на эту тему — см. каталог \chapt11\articles\ на прилагаемом компакт-диске.

Прежде всего

Для изучения материалов этой главы необходимо;

- установить на компьютер Windows 2000 Server;
- выполнить упражнения предыдущих глав.

Занятие 1. Инфраструктура открытого ключа

Шифрование открытым ключом — технология, чрезвычайно важная для защиты электронной коммерции, внутренних и внешних сетей, а также Web-приложений. Впрочем, чтобы задействовать преимущества шифрования открытым ключом, требуется соответствующая инфраструктура. Windows 2000 включает в себя собственную инфраструктуру открытого ключа (PK1), спроектированную с учетом всех преимуществ архитектуры защиты этой ОС. На этом занятии дан обзор PKI в Windows 2000 и обсуждаются характеристики системы безопасности, шифрования, сертификатов и служб Microsoft Certificate Services.

Изучив материал этого занятия. Вы сможете:

- ✓ описать базовые концепции шифрования открытым ключом и реализацию PKI в Windows 2000;
- ✓ выполнять запросы сертификатов и добавлять центры сертификации (certificate authorities, CA);
- ✓ устанавливать службы Microsoft Certificate Services.

Продолжительность занятия - около 35 минут.

Составляющие безопасности

Компьютерная безопасность включает все: от аппаратно-технической части до ПО. В программной области система безопасности должна выполнять 4 функции: *аутентификацию* (authentication), *проверку целостности* (integrity), *конфиденциальность* (confidentiality) и *предотвращение повторов* (anti-replay).

Аутентификация

Это процесс надежного определения подлинности подключающегося компьютера или пользователя. Аутентификация (проверка подлинности) базируется на криптографии и гарантирует, что подключившиеся к сети злоумышленники не получат информацию, посредством которой они смогут выдать себя за зарегистрированного пользователя. Она позволяет подключающимся лицам доказывать свою подлинность другим лицам, прежде чем незащищенные данные будут переданы по сети. Без достоверной аутентификации любые данные и компьютер, с которого они получены, считаются подозрительными.

Целостность

Подразумевает сохранение информации в том виде, в котором она была передана. Службы обеспечения целостности защищают данные от неавторизованной модификации при передаче. Без обеспечения целостности любая информация и компьютер, с которого она получена, считаются подозрительными.

Конфиденциальность

Гарантирует, что передаваемые данные будут доступны только уполномоченным адресатам.

Предотвращение повторов

Подразумевает, что дейтаграммы передаются однократно. Каждая посланная дейтаграмма уникальна. Эта уникальность предотвращает атаки, в которых сообщения перехватываются и затем повторно используются для несанкционированного доступа к информации.

Криптография

Это набор математических методов для шифрования и расшифровки данных. Шифрование позволяет надежно передавать конфиденциальные данные — они не будут доступны неуполномоченным лицам. В криптографии применяются ключи в сочетании с алгоритмами для защиты данных. *Ключ* (key) — это некое число, используемое в ходе шифрования и расшифровки информации. Даже если алгоритм известен, безопасность не ставится под угрозу, потому что прочитать данные без ключа невозможно. Например, алгоритм работы кодового замка известен всем: чтобы его открыть, достаточно набрать соответствующий код. Однако ключ к замку — цифры в комбинации кода — является тайной и известен только лицу, знающему комбинацию. Иными словами, безопасность обеспечивается не алгоритмом, а ключом. Алгоритм создает инфраструктуру, в которой применяется ключ. Системы безопасности основаны на шифровании открытым или закрытым ключами — подробнее об этом Вы узнаете ниже.

Существует много алгоритмов шифрования, каждый из которых выполняет различные операции по защите. Вот некоторые из них.

Алгоритм	Описание
Rivest, Shamir. Adleman (RSA)	Базовый алгоритм шифрования, поддерживающий цифровые подписи, распределенную аутентификацию, прием закрытого ключа с помощью открытого, шифрование больших объемов данных без предварительной передачи секретной информации.
Digital Signature Standard (DSA)	Алгоритм шифрования с применением открытого ключа для генерации цифровых подписей.
Diffie-Hellman	Алгоритм шифрования с применением открытого ключа, позволяющий двум связывающимся сторонам использовать общий ключ без применения шифрования во время генерации ключа.
Hash Message Authentication Code (HMAC)	Алгоритм шифрования с применением закрытого ключа, обеспечивающий целостность, аутентификацию и предотвращение повторов. HMAC использует хеш-функции совместно с закрытым ключом. Для создания и проверки цифровой подписи применяется хеш-код, или *выборка сообщения* (message digest).
HMAC-Message Digest function 5 (MD5)	Хеш-функция, генерирующая 128-разрядное число — цифровую подпись. Применяется для аутентификации, проверки целостности и предотвращения повторов.
HMAC-Secure and Hash Algorithm (SHA)	Хеш-функция, генерирующая 160-разрядную цифровую подпись для аутентификации, проверки целостности и предотвращения повторов.
Data Encryption Standard-Cipher Chaining (DES-CBC)	Алгоритм шифрования с применением закрытого ключа. Генерируемое случайное число используется совместно с закрытым ключом для шифрования информации.

Шифрование с применением открытых ключей

Представляет собой асимметричную схему шифрования с парой ключей. Называется асимметричной, так как использует два математически связанных парных шифровальных ключа — открытый и закрытый. Для шифрования открытым ключом объект (например пользователь) должен сгенерировать оба парных ключа. Каждый объект будет иметь толь-

ко один (собственный) закрытый ключ, но сможет получать множество открытых ключей, парных к другим закрытым ключам, Объекты получают открытые ключи одним из двух способов:

- владелец закрытого ключа посылает адресату соответствующий открытый ключ;
- адресат получает такой ключ из службы каталогов, например из Active Directory или DNS.

Открытый и закрытый ключи обычно применяются для шифрования данных и цифровой подписи сообщения.

Шифрование данных

Обеспечивает конфиденциальность, гарантируя, что только указанный получатель сможет расшифровать и просмотреть исходные данные. Для передачи секретной информации отправитель сначала получает открытый ключ получателя. Затем на основе этого открытого ключа получатель шифрует и передает данные. Полученную информацию адресат расшифровывает, используя свой закрытый ключ. Шифрование надежно, только если отправитель применяет для кодирования открытый ключ получателя. Если для шифрования отправитель использует собственный закрытый ключ, то кто угодно сможет перехватить данные и расшифровать по открытому ключу отправителя.

Цифровая подпись

Обеспечивает аутентификацию и проверку целостности, но не конфиденциальности данных. Позволяет получателю удостовериться в подлинности отправителя и проверяет, что содержимое не изменялось при передаче. Препятствует попыткам послать сообщение от имени другого лица.

При отправлении сообщения создается его выборка — представление сообщения вроде *контрольной суммы* (cyclic redundancy check, CRC), Для зашифровки выборки сообщения отправитель применяет свой закрытый ключ. Принимая сообщение, адресат получает открытый ключ отправителя для расшифровки выборки сообщения. Затем он создает выборку из полученного сообщения и сравнивает ее с расшифрованной выборкой. Если они совпадают, целостность гарантирована (рис. 11-1).

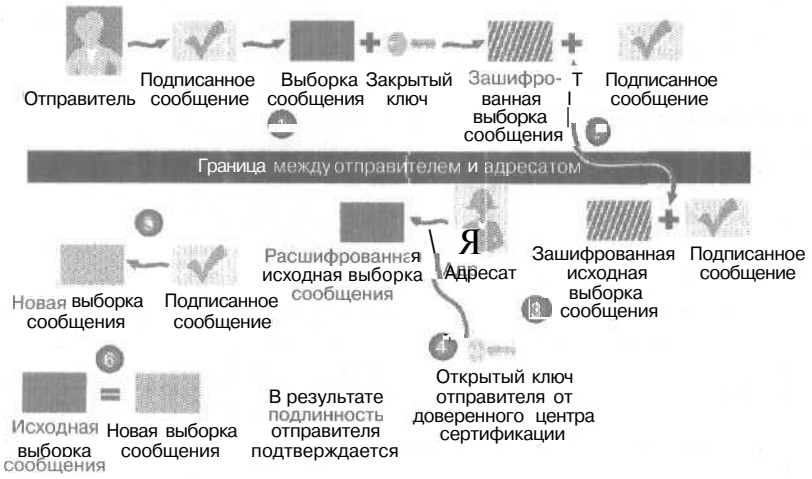


Рис. 11-1. Использование подписи сообщения, его выборки и PKI для проверки подлинности отправителя

Аутентификация обеспечивается тем, что ключи составляют пару. Так как выборка сообщения была зашифрована закрытым ключом отправителя (и только его открытый ключ позволяет ее расшифровать), получатель может быть уверен, что сообщение пришло именно от владельца этой пары ключей. Впрочем, получатель должен иметь возможность удостовериться, что эти ключи принадлежат истинному отправителю, а не тому, кто выдает себя за него. Это обеспечивает выпускаемый доверяемой третьей стороной сертификат, подтверждающий подлинность обладателя открытого ключа. Об этой третьей стороне — *центре сертификации* (Certificate Authority, CA) — см. ниже.

Секретные ключи

Секретный ключ (или *общий секретный ключ*) применяется во многом подобно открытому ключу, однако в этом случае существует только один ключ — он-то и обеспечивает защиту. Секретный ключ обычно используется в особых сеансах связи или на короткое время, после чего аннулируется. Этот процесс имеет преимущества над открытыми ключами. Например, если посторонний узнает такой ключ, он в принципе сможет подключиться к сеансу связи. И все же злоумышленник не сможет выдать себя за определенного пользователя или конкретный компьютер вне этого сеанса связи и не сможет, применив этот секретный ключ, получить доступ к остальным ресурсам.

Для безопасной доставки общего секретного ключа обеим сторонам нужен соответствующий механизм. Если ключ просто переслать по сети, любой злоумышленник без труда его перехватит.

Обмен секретным ключом

Доставка секретного ключа обеим сторонам обычно выполняется с применением открытых ключей. Они позволяют зашифровать секретный ключ перед его пересылкой по сети. Открытые ключи обеспечивают конфиденциальность, аутентификацию и целостность данных; следовательно, безопасность при пересылке секретного ключа не нарушается.

Например, если Алексей хочет послать данные Максиму, используя секретный ключ, то оба сначала генерируют по половине этого ключа. Алексей получает открытый ключ Максима, шифрует свою половину секретного ключа и отсылает ее Максиму. Точно так же Максим получает открытый ключ Алексея, шифрует свою половину секретного ключа и отсылает ее Алексею. Затем оба соединяют половины секретного ключа и получают общий ключ для шифрования пересылаемых данных (рис. 11-2). Это обеспечивает аутентификацию, целостность данных и конфиденциальность.

Шифрование данных

Для обеспечения конфиденциальности данные должны быть зашифрованы обшим секретным ключом. Поскольку теперь используется только один ключ, известный и отправителю, и получателю, процесс шифрования упрощается. Отправитель шифрует данные общим секретным ключом, а получатель им же их и расшифровывает. Так как никто более в сети не знает этого секретного ключа, данные защищены от взлома. Обычно отправитель и получатель аннулируют секретный ключ сразу после сеанса связи.

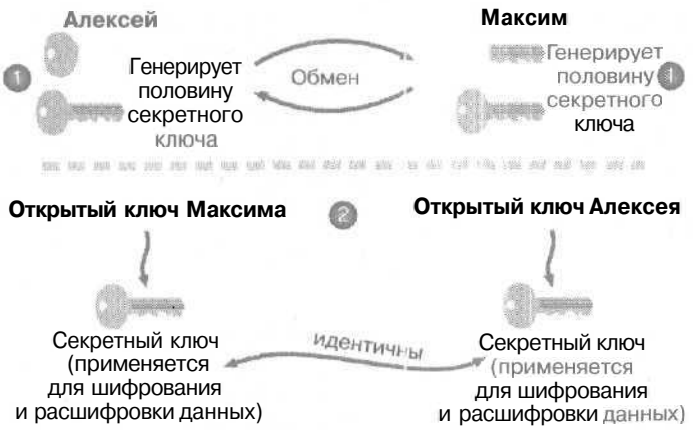


Рис. 11-2. Обмен секретным ключом, при котором Алексей и Максим генерируют каждый по половине секретного ключа для создания общего секретного ключа

Сертификаты

Шифрование открытым ключом подразумевает, что подлинность владельца обоих ключей установлена достоверно. *Цифровой сертификат* (или просто *сертификат*) — это набор данных, полностью идентифицирующих сущность. Некий доверенный *центр сертификации* (Certificate Authority, CA) выпускает сертификаты после проверки подлинности удостоверяемого лица. Центр сертификации (ЦС) является для двух сообщающихся сторон доверяемой третьей стороной.

Например, если Алексей хочет послать заверенные данные Максиму, он посылает ему свой открытый ключ. Доверенный ЦС удостоверяет открытый ключ Алексея, подтверждая тем самым подлинность его личности. Поскольку Максим доверяет ЦС, он доверяет и Алексею.

Этот процесс сходен с тем, что происходит у нотариуса, Лицо подписывает документ в присутствии нотариуса и предъявляет удостоверение личности. Нотариус является заслуживающим доверия лицом, так что каждый, кто проверяет документ, может быть уверен, что подпись на нем подлинна. Аналогично, когда отправитель подписывает сообщение закрытым ключом, получатель сообщения может, используя открытый ключ отправителя, заверенный ЦС, проверить подлинность отправителя. Поскольку ЦС удостоверяет открытый ключ, получатель может быть уверен в подлинности отправителя. Доверенный ЦС может быть сторонним поставщиком сертификатов, таким как VeriSign или Microsoft Certificate Services.

Например, пользователь может получить цифровой сертификат для отправки сообщений по электронной почте. Такой сертификат включает в себя открытый ключ и сведения об авторе сообщения. В посылаемое сообщение включается цифровая подпись, в которой используется открытый ключ. Получатель принимает открытый ключ и удостоверяется в подлинности отправителя. Адресату личный ключ никогда не посылается.

Стандарт X.509

Определяет синтаксис и формат сертификата. В Windows 2000 процессы, связанные с сертификатами, опираются на стандарт *X.509*. Так как сертификаты применяются в разных целях (например для шифрования электронной почты или файловой системы), каждый сертификат заключает в себе разную информацию. Впрочем, сертификат должен обязательно включать:

- номер версии;
- серийный номер;
- идентификатор алгоритма подписи;
- имя издателя;
- срок действия;
- имя субъекта (пользователя);
- информацию об открытом ключе субъекта;
- уникальный идентификатор издателя;
- уникальный идентификатор субъекта;
- расширения;
- цифровую подпись поставщика, заверяющую действительность связи между открытым ключом субъекта и сведениями для его идентификации.

Списки отзыва сертификатов

Сертификаты, как и большинство удостоверений в обычной жизни, могут терять силу и становиться недействительными. ЦС также вправе отозвать сертификат по какой-либо причине. С этой целью ЦС ведет *список отзыва сертификатов* (certificate revocation list, CRL). Он доступен пользователям сети, и они могут определять действительность любого конкретного сертификата.

Иерархия ЦС

Обычно один ЦС не применяется для аутентификации всей интрасети — удобнее, чтобы одни ЦС могли сертифицировать остальные. В результате пользователи будут доверять какому-либо одному ЦС вместо того, чтобы доверять всем ЦС. Иерархия ЦС дает следующие преимущества:

- **гибкость** — легко перемещать, отзывать или связывать ЦС, не затрагивая остальные части организации;
- **распределенное администрирование** — администраторы несут ответственность только за собственные сайты;
- **собственные политики безопасности** — у каждого центра ЦС может быть своя политика безопасности.

ЦС на вершине иерархической цепочки называется корневым, нижележащие — *промежуточными* (intermediate), *подчиненными* (subordinate) или *издающими* (issuing).

Службы сертификации

Службы Microsoft Certificate Services позволяют организации управлять изданием, обновлением и отзывом цифровых сертификатов, не обращаясь к внешним ЦС. Вдобавок они позволяют в полной мере управлять действиями по изданию, поддержке и отзыву сертификатов, контролировать формат и содержание самих сертификатов. Наконец, они протоколируют все операции, позволяя администратору отслеживать, проверять и управлять запросами сертификатов.

Возможности служб сертификации

Службы Microsoft Certificate Services предоставляют широкие возможности для организаций, которые не хотели бы обращаться к сторонним ЦС и которым нужен адаптируемый механизм аутентификации.

Независимость от политики

Для получения сертификата заказчик должен соответствовать определенным требованиям. Эти требования закладываются в политике сертификации. Например, в одном случае

сертификат выдается, только если заказчики лично представят удостоверяющие документы, а в другом — удостоверение выдается на основании запросов по электронной почте.

Политика реализуется в соответствующих компонентах, написанных на языках Java, Visual Basic или Microsoft C/C++. Стандартная политика служб сертификации позволяет пользователю запрашивать сертификаты через страницу HTML.

Независимость от способа передачи

Службы сертификации могут запрашивать и рассылать сертификаты посредством любого транспорта. Они вправе принимать запросы сертификата от любого заказчика я высылать ему сертификаты по протоколу HTTP, путем *удаленного вызова процедур* (remote procedure call, RPC), публикации в файловой системе или иначе.

***Соответствие** стандартам*

Службы сертификации:

- принимают запросы, соответствующие стандарту Public Key Cryptography Standards (PKCS) #10;
- поддерживают данные, подписанные по стандарту PKCS #7;
- издают сертификаты по стандарту X.509 версий 1.0 и 3.0.

Службы сертификации способны поддерживать и дополнительные форматы сертификатов, а также включают в себя компонент LDAP, т. е. интегрированы в Active Directory.

Управление ключами

Безопасность системы сертификатов зависит от защищенности закрытых ключей. Службы сертификации не позволяют получить несанкционированный доступ к закрытому ключу. Для управления ключами и выполнения других криптографических задач по построению безопасного хранилища сертификатов службы сертификации применяют интерфейс Microsoft CryptoAPI.

Архитектура служб сертификации

Включает серверное ядро, обрабатывающее запросы сертификатов и управляющее дополнительными модулями (рис. 11-3).

Рис. 11-3. Схема взаимодействия компонентов служб сертификации

Серверное ядро

Этот главный компонент служб сертификации выступает как посредник для всех запросов, получаемых от входных модулей, направляя потоки информации между компонентами во время обработки запроса и генерации сертификата. На каждой стадии обработки ядро взаимодействует с различными модулями, чтобы выполнять действия, соответствующие состоянию запроса.

Посредник

Этот архитектурный компонент получает запросы новых сертификатов от клиентов и направляет их серверному ядру. Посредник состоит из двух частей: приложения-посредника, выполняющего действия от имени клиента, и клиентского интерфейса, осуществляющего обмен информацией между приложением-посредником и серверным ядром.

Приложения-посредники могут предусматривать обработку запросов сертификатов от разных типов клиентов, использующих несколько механизмов передачи или соответствующих критериям определенной политики. Приложение-посредник Microsoft Internet Information Services (IIS) обслуживает клиентов через протокол HTTP. Такие приложения также проверяют состояние направленного ранее запроса и получают сведения о конфигурации служб сертификации.

База данных сервера

Службы сертификации включают в себя БД, которая хранит информацию о текущем состоянии и журнал со всеми выпущенными сертификатами и списками отзыва сертификатов (CRL). Эта БД состоит из журнала и очереди запросов.

Журнал

В журнале регистрируется информация обо всех выпущенных сервером сертификатах и CRL, так что администраторы могут отслеживать, проверять и архивировать сведения о деятельности сервера. Этот журнал также используется серверным ядром для хранения данных по планируемым отзывам до их опубликования в CRL. Кроме того, в журнале содержатся невыполненные почему-либо запросы сертификатов.

Очередь запросов

Содержит сведения о ходе обработки сервером запроса сертификата: получении, анализе, авторизации, подписи и отправке.

Модуль политики

Содержит набор правил, обусловливающих выпуск, обновление и отзыв сертификатов. Все получаемые ядром запросы предаются модулю политики для проверки. Он также применяется для анализа дополнительной информации, содержащейся в запросе, и соответствующей настройки параметров сертификата.

Обработчики расширений

Работают в тандеме с модулем политики для настройки пользовательских расширений сертификата. Каждый такой обработчик выступает как шаблон для расширения, которое должно быть отражено в сертификате. При необходимости модуль политики подгружает соответствующий обработчик.

Модули выхода

Публикуют готовый сертификат и CRL, используя любые транспорты и протоколы. По умолчанию при выпуске сертификата или CRL информация выдается на каждый модуль выхода, установленный на сервере.

Службы сертификации поддерживают интерфейс COM для создания дополнительных модулей выхода, адаптированных под разные транспорты и протоколы или иные способы доставки. Например, модуль выхода LDAP может быть использован для опубликования в службе каталогов только сертификатов клиентов, но не сертификатов сервера. При этом модуль выхода может использовать COM-интерфейс для определения типа сертификата, выпускаемого сервером, и отфильтровывать все неподходящие (серверные) сертификаты.

Обработка запроса сертификата

Службы сертификации включают средства обработки запросов сертификатов и выпуска цифровых сертификатов (рис. 11-4).

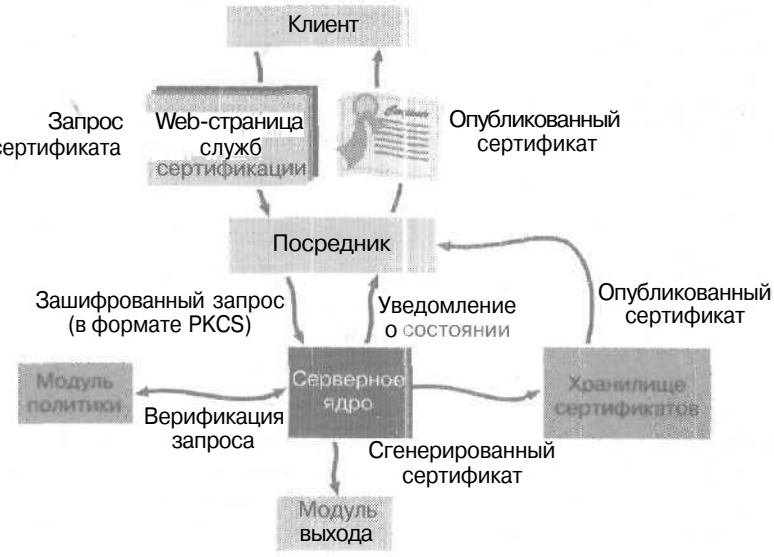


Рис. 11-4. Обработка запроса сертификата

При обработке запроса службы сертификации выполняют следующие действия.

1. Клиент направляет запрос сертификата приложению-посреднику. Это приложение транслирует его в формат PKCS #10 и пересылает в ядро.
2. Ядро вызывает модуль политики, который определяет свойства запроса, авторизован он или нет, и настраивает необязательные свойства сертификата.
3. Если запрос утвержден, ядро обрабатывает запрос и генерирует сертификат.
4. Ядро сохраняет сертификат в хранилище и передает сведения о состоянии запроса приложению-посреднику. Если при этом требуется модуль выхода, ядро сообщает ему о выпуске сертификата. Это разрешает модулю выхода выполнить дальнейшие операции, например опубликовать сертификат в службе каталогов.
5. Приложение-посредник получает выпущенный сертификат из хранилища сертификатов и пересылает его клиенту.

Установка цифрового сертификата

Этот процесс начинается с клиентского запроса сертификата и кончается установкой выпущенного сертификата в приложение клиента. Для установки сертификата на клиентской системе используется Web-страница *http://имя_сервера/certsrv*.

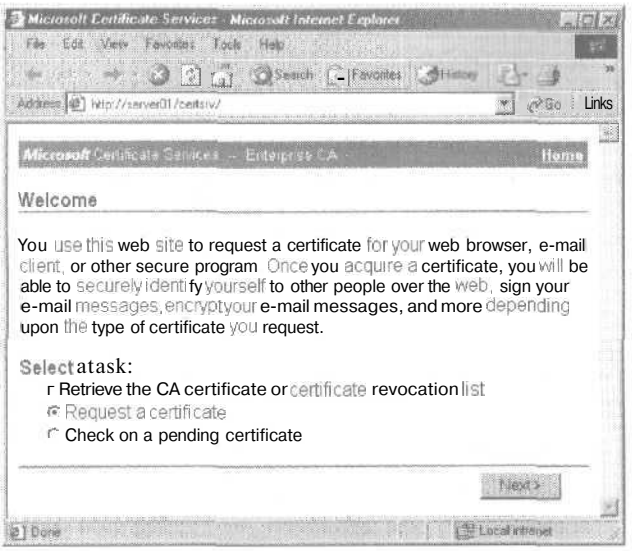


Рис. 11-5. Web-страница работы с сертификатами на Server01

Сертификаты ЦС

В процессе выпуска цифрового сертификата ЦС подтверждает подлинность лица, запрашивающего сертификат, и затем подписывает этот сертификат собственным закрытым ключом.

Клиентское приложение, например Microsoft Internet Explorer, проверяет подпись ЦС перед принятием сертификата. Если подпись ЦС недействительна или поступила из неизвестного источника, Internet Explorer выводит предупреждение и позволяет отказаться от сомнительного сертификата.

Примечание Если в Internet Explorer применяется низкий уровень безопасности, сообщение о недействительных сертификатах может не появиться. Низкий уровень безопасности приемлем в абсолютно доверенных интрасетях, но не для доступа в Интернет.

Кроме сертификатов, подтверждающих подлинность сервера и клиента, существуют сертификаты, идентифицирующие сами ЦС.

Сертификат ЦС содержит открытый ключ для проверки цифровых подписей и идентифицирует ЦС, выпустивший сертификаты для запросивших их серверов и клиентов. Клиенты используют сертификат ЦС для проверки сертификата сервера и наоборот.

Сертификат, выданный ЦС самому себе, называется корневым, так как является сертификатом для корневого ЦС. Последний заверяет собственный сертификат, поскольку по определению для него не существует вышестоящего центра сертификации.

Распространение и установка сертификатов ЦС

Сертификаты ЦС запрашиваются и выпускаются иначе, чем сертификаты для серверов или клиентов. Сертификаты сервера или клиента уникальны для каждого их заказчика и не поступают в общее пользование — они должны генерироваться и выпускаться ЦС по требованию. Сертификат ЦС, напротив, не требует выпуска по запросу. Он создается однократно и потом предоставляется для доступа всем серверам или клиентам, запрашивающим сертификаты у ЦС.

Обычно сертификаты ЦС хранятся в месте, известном и доступном всем заказчикам сертификатов.

Установка служб сертификации

Для установки служб сертификации дважды щелкните значок Add/Remove Programs (Установка и удаление программ) на панели управления Windows или выберите соответствующий необязательный компонент на этапе установки Windows 2000 Server. Если Вы знакомы с созданием ЦС, Вы можете настроить дополнительные параметры при установке Certificate Services.

Тип ЦС

Определяет, как ЦС будет использоваться в иерархии и будет ли он обращаться к Active Directory. Существуют следующие типы центров сертификации:

- **корневой ЦС предприятия** — корневой ЦС для иерархии, требует для своей работы Active Directory;
- подчиненный ЦС предприятия — подчиненный корневого ЦС предприятия, также требует Active Directory; этот ЦС будет запрашивать сертификаты у своего корневого ЦС;
- изолированный корневой ЦС — корневой ЦС для иерархии, не требующий Active Directory;
- **изолированный подчиненный ЦС** — подчиненный корневого ЦС, не требующий Active Directory; этот ЦС будет запрашивать сертификаты у своего отдельного корневого ЦС.

Службы сертификации, установленные в качестве ЦС предприятия, будут публиковать сертификаты в Active Directory. Поставщики безопасности, например Kerberos, могут запрашивать Active Directory для получения сертификата, содержащего открытый ключ.

Информация о ЦС

Вы должны предоставить сведения об исходном ЦС, созданном при установке служб сертификации, например имя ЦС. Информацию об установленном ЦС изменить нельзя.

Дополнительные настройки

Позволяют выбрать тип алгоритмов шифрования, которые будет использовать новый ЦС. Вы вправе также задать имя поставщика службы шифрования, алгоритм хеширования, длину ключа и возможность применения имеющихся открытых и закрытых ключей.

Администрирование служб сертификации

Основным инструментом здесь является оснастка Certification Authority (рис. 11-6).

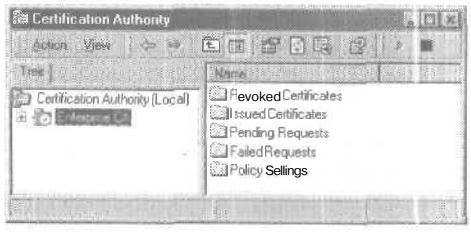


Рис. 11-6. Представление ЦС предприятия в оснастке Certification Authority (Центр сертификации)

Эта оснастка позволяет администратору:

- запускать и останавливать службы сертификации;
- настраивать разрешения и делегировать управление ЦС;

- просматривать сертификат ЦС;
- выполнять резервное копирование ЦС;
- восстанавливать ЦС из резервной копии;
- обновлять корневой ЦС;
- обновлять подчиненный ЦС;
- управлять отзывом сертификатов;
- управлять запросами сертификатов;
- управлять шаблонами сертификатов;
- изменять параметры политики;
- проецировать сертификат на учетную запись пользователя;
- модифицировать модуль политики и модуль выхода.

Оснастка Certification Authority (Центр сертификации) позволяет администрировать ЦС на локальном или удаленном компьютере. Она устанавливается со службами сертификации или с пакетом дополнительных средств администрирования (см. главу 6).

Для администрирования служб сертификации также применяется утилита командной строки certutil.exe. Запущенная без параметров, она выведет сводную информацию о локальном ЦС. Эта утилита применяется для вывода сведений о конфигурации ЦС, настройки служб сертификации, резервного копирования и восстановления компонентов ЦС, для проверки сертификатов, пар ключей и цепочек сертификатов.

Если Вам нужно защитить Web-страницы ЦС, задействуйте Internet Information Services. В дереве консоли раскройте папку Default Web Site (Веб-узел по умолчанию) и выберите папку CertSrv. В меню Action (Действие) выберите команду Properties (Свойства), В открывшемся окне на вкладке Directory Security (Безопасность каталога) в области Anonymous access and authentication control (Анонимный доступ и проверка подлинности) щелкните кнопку Edit (Изменить), В диалоговом окне Authentication Methods (Способы проверки подлинности) задайте параметры безопасности для Web-страниц ЦС.

Упражнение 1: установка и конфигурирование служб сертификации

Установите корневой ЦС предприятия и с его помощью выпустите, установите и отзовите несколько сертификатов. Рекомендуется всегда создавать корневой ЦС, который будет лишь генерировать сертификаты для подчиненных ЦС. А они в свою очередь будут выпускать сертификаты для конкретных целей — обслуживания приложений и аутентификации. Применять главный ЦС для этих целей небезопасно, так как при нарушении его зашиты все выпущенные сертификаты будут скомпрометированы. Впрочем, для обучения установке и конфигурированию достаточно настроить только корневой ЦС.

► Задание 1: установите службы сертификации и сконфигурируйте ЦС

Установите службы сертификации на Server01. Он будет выполнять роль корневого ЦС предприятия.

1. Зарегистрируйтесь на ServerOl как Administrator с паролем password.
2. Раскройте меню Start\Settings (Пуск\Настройка) и щелкните ярлык Control Panel (Панель управления).

   Откроется окно Control Panel (Панель управления).
3. Дважды щелкните значок Add/Remove Programs (Установка и удаление программ).

   Откроется одноименное окно.
4. На левой панели шелкните значок Add/Remove Windows components (Добавление и удаление компонентов Windows).

Откроется окно мастера компонентов Windows.

5. Пометьте флажок Certificate Services (Службы сертификации).

   Появится сообщение, что после установки служб сертификации данный компьютер не сможет быть переименован, включен в домен или удален из его состава.

6. Щелкните кнопку Yes (Да).
7. В окне Windows Components (Компоненты Windows) щелкните кнопку Details (Состав).

   Откроется окно Certificate Services (Службы сертификации).

   Дополнительные компоненты включают как службу для создания ЦС, так и регистрационную Web-форму для запросов и получения сертификатов от ЦС.

8. Щелкните кнопку OK.
9. В окне Windows Components (Компоненты Windows) щелкните кнопку Next (Далее).

   Откроется окно Certification Authority Type (Тип центра сертификации).

10. Выберите последовательно каждый переключатель и изучите описание каждого типа ЦС.

    Заметьте: ЦС предприятия можно установить, только если на сервере установлены службы Active Directory. Изолированный ЦС не зависит от Active Directory, хотя, если эта служба каталогов установлена, будет к ней обращаться. Подчиненный ЦС можно создать только при наличии вышестоящего ЦС.

11. Щелкните переключатель Enterprise Root CA (корневой ЦС предприятия), пометьте флажок Advanced Options (Дополнительные возможности) и щелкните кнопку Next (Далее).

    Откроется окно Public and Private Key Pair (Пара из открытого и закрытого ключей). На Ваш выбор предлагается несколько *поставщиков служб шифрования* (Cryptographic Service Providers, CSP), каждый из которых имеет один или несколько алгоритмов хеширования для генерации пар ключей. Здесь же Вы можете задать длину ключа или применить существующий ключ, установленный на компьютере, а также импортировать ключи и просматривать сертификаты.

12. Убедитесь, что в списке CSP (Поставщик CSP) выбран пункт Microsoft Base Cryptographic Provider v1.0, в списке Hash Algorithm (Алгоритм хеширования) — SHA-1, а в списке Key Length (Длина ключа) — Default (По умолчанию). Щелкните кнопку Next (Далее).

    Откроется окно CA Identifying Information (Сведения о центре сертификации).

13. Введите данные из таблицы в текстовые поля этого окна:

Поле	Вводимое значение
CA name (Имя ЦС)	Enterprise CA
Organization (Организация)	Microsoft Corporation
Organizational unit (Подразделение)	Microsoft Press
City (Город)	Redmond
State or province (Область)	Washington
E-mail (**Электронная** почта)	ca-mp@microsoft.com
CA description (Описание ЦС)	Root CA for self-study training only

    Заметьте: данный сертификат будет иметь силу в течение двух лет.

14. Щелкните кнопку Next (Далее).

    Откроется окно Data Storage Location (Размещение хранилища данных).

По умолчанию БД сертификатов и ее журнал CertLog помещаются в загрузочном разделе диска. Если его емкость невелика, укажите другой защищенный раздел.

Флажок Store configuration information in a shared folder (Сохранить сведения о конфигурации в общей папке) не имеет значения, если на компьютере есть Active Directory и компьютер, работающий как ЦС, входит в какой-либо домен. Информация о конфигурации данного ЦС автоматически публикуется в хранилище Active Directory.

15. Щелкните кнопку Next (Далее).

Появится сообщение, что в данный момент работает служба IIS и для продолжения установки надо завершить работу этой службы.

16. Щелкните кнопку OK.

Откроется окно Configuring Components (Настройка компонентов), а затем — окно Completing the Windows Components Wizard (Завершение работы мастера компонентов Windows).

17. Щелкните кнопку Finish (Готово), а затем в окне Add/Remove Programs — кнопку Close (Закрыть).
18. Закройте окно Control Panel.

▶ Задание 2: сгенерируйте, установите и отзовите сертификат для Server01

Задействуйте Web-страницу работы с сертификатами и оснастку Certificate Authority (Центр сертификации).

1. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык Certification Authority (Центр сертификации).

Откроется оснастка Certification Authority (Центр сертификации).

2. В дереве консоли раскройте узел Enterprise CA.
3. Выберите папку Pending Requests (Запросы в ожидании) и сверните окно оснастки.
4. В меню Start (Пуск) и выберите команду Run (Выполнить).

Откроется диалоговое окно Run (Запуск программы).

5. В поле Open (Открыть) наберите **http://server01/certsrv** и щелкните кнопку OK.

Откроется окно мастера подключения к Интернету.

6. Выберите способ подключения — I Connect Through A Local Area Network (LAN) (С помощью локальной сети). Затем щелкните кнопку Next (Далее).

Откроется окно Local Area Network Internet Configuration (Параметры Интернета для локальной сети).

7. Сбросьте флажок Automatic Discovery Of Proxy Server (Recommended) (Автоматическое определение прокси-сервера) и щелкните кнопку Next (Далее).

Откроется окно Set Up Your Internet Mail Account (Настройте учетную запись почты Интернета).

8. Щелкните переключатель No (Нет), а затем — кнопку Next (Далее).

Откроется окно Completing The Internet Connection (Завершение настройки).

9. Щелкните кнопку Finish (Готово).

В Internet Explorer откроется страница работы с сертификатами.

10. Изучите информацию на этой странице и убедитесь, что выбран переключатель Request A Certificate (Запросить сертификат).
11. Щелкните кнопку Next (Далее).

Откроется страница Choose Request Type (Выбор типа запроса) с выбранным пунктом User Certificate Request (Запрос сертификата пользователя).

12. Щелкните кнопку Next (Далее).

    Откроется страница User Certificate — Identifying Information (Сертификат программы обзора веба — Идентифицирующая информация).

13. Заполните два первых поля и щелкните кнопку More Options (Дополнительные параметры).

    Заметьте: выбран тот тип CSP, который Вы задали при установке служб сертификации.

14. Щелкните кнопку Submit (Выдать запрос).
15. Щелкните ссылку Home (Домой), чтобы вернуться на основную страницу работы с сертификатами.
16. Сверните окно Internet Explorer и восстановите окно оснастки Certification Authority (Центр сертификации).

    На правой панели оснастки появится Ваш запрос сертификата. Если Вы не увидите его, нажмите клавишу F5, чтобы обновить содержимое панели.

17. Щелкните значок запроса правой кнопкой, в контекстном меню выберите All Tasks (Все задачи), затем — команду Issue (Выдать).
18. В дереве консоли выберите папку Issued Certificates (Выданные сертификаты). На правой панели оснастки появится Ваш сертификат. Если Вы не увидите его, нажмите клавишу F5, чтобы обновить содержимое панели.
19. Дважды щелкните этот сертификат.

    Откроется окно Certificate (Сертификат) с тремя вкладками.

20. Перейдите на вкладку Details (Состав).
21. В списке под раскрывающимся списком Show (Показать) щелкните строку Issuer (Поставщик).

    В нижнем текстовой области будут отражены сведения, которые Вы ввели в окне CA Identifying Information.

22. Щелкните кнопку OK, чтобы закрыть окно свойств сертификата.
23. Сверните окно оснастки Certification Authority и восстановите окно Internet Explorer.
24. Щелкните переключатель Check on a pending certificate (Проверить ожидающий выполнения запрос на сертификат), а затем — кнопку Next (Далее).

    Откроется страница с информацией об ожидающих выполнения запросах сертификатов.

25. Щелкните кнопку Next (Далее).

    Откроется страница Certificate Issued (Сертификат выдан).

26. Щелкните ссылку Install This Certificate (Установить этот сертификат).

    Откроется страница Certificate Installed (Сертификат установлен).

27. Закройте Internet Explorer.
28. Восстановите окно оснастки Certification Authority (Центр сертификации) и в ее правой панели выберите Ваш сертификат.
29. В меню Action (Действие) выберите All Tasks (Все задачи), а затем — команду Revoke Certificate (Отзыв сертификата).

    Откроется диалоговое окно Certificate Revocation (Отзыв сертификатов).

30. В списке Reason Code выберите Key Compromise (Компрометация ключа) и щелкните кнопку Yes (Да).
31. В дереве консоли щелкните папку Revoked Certificates (Отозванные сертификаты).

    Отозванный сертификат появится на правой панели.

32. В *меню* Action (Действие) выберите All Tasks (Все задачи), а затем — команду Publish (Публикация).

Диалоговое окно Certificate Revocation List (Список отзыва сертификатов) сообщит, что предыдущий список еще действителен.

33. Щелкните кнопку Yes (Да).
34. Закройте оснастку Certification Authority (Центр сертификации).
35. В меню Start (Пуск) выберите команду Run (Выполнить).

    Откроется окно Run (Запуск программы), где в поле Open (Открыть) уже будет набрана ссылка на каталог Certsrv.
36. Щелкните кнопку OK.

    В Internet Explorer будет открыта страница работы с сертификатами.
37. Щелкните переключатель Retrieve The CA Certificate Or Certificate Revocation List (Получить сертификат ЦС или список отзыва сертификатов), а затем — кнопку Next (Далее).
38. На открывшейся странице щелкните ссылку Download Latest Certificate Revocation List (Загрузить последний список отзыва сертификатов).

    Откроется диалоговое окно File Download (Загрузка файла).
39. Щелкните переключатель Open This File From Its Current Location (Открыть этот файл из текущего места), а затем — кнопку OK.

    Откроется диалоговое окно Certificate Revocation List (Список отзыва сертификатов).
40. Перейдите на вкладку Revocation List (Список отзыва).
41. В списке Revoked Certificates (Отозванные сертификаты) щелкните отозванный сертификат.

    В списке ниже отобразится серийный номер сертификата, дата и причина отзыва.
42. Щелкните кнопку OK, чтобы закрыть окно Certificate Revocation List (Список отзыва сертификатов).
43. Закройте Internet Explorer.

Резюме

Windows 2000 включает собственную инфраструктуру открытого ключа, в полной мере использующую все особенности архитектуры системы безопасности этой ОС. Шифрование открытым ключом — это асимметричная схема с применением пары ключей (открытого и закрытого). Владелец пары ключей идентифицируется с помощью цифровых сертификатов. Обработка сертификатов в Windows 2000 основана на стандарте X.509. Службы сертификации позволяют организации управлять выпуском, установкой и отзывом цифровых сертификатов без обращения к внешним центрам сертификации. Службы сертификации не зависят от политики безопасности и способа передачи, соответствуют открытым стандартам и обеспечивают управление ключами. Архитектура служб сертификации включает серверное ядро, обрабатывающее запросы сертификатов, и другие взаимодействующие с ним модули. Службы сертификации устанавливаются с помощью утилиты Add/Remove Programs (Установка и удаление программ) из панели управления или на этапе установки Windows 2000 Server как необязательный компонент. Для администрирования служб сертификации применяется оснастка Certification Authority (Центр сертификации), утилита Certutil и Web-страница работы с сертификатами.

Занятие 2. Технологии открытого ключа

Windows 2000 поддерживает технологии, основанные на шифровании открытым ключом: защищенные каналы, смарт-карты, Authenticode, *шифрованную файловую систему* (Encrypting File System, EFS) и Internet Protocol Security (IPSec). Здесь приведен обзор этих технологий и поясняется, как они вписываются в PKI.

Изучив материал этого занятия, Вы сможете:

- ✓ описать базовые компоненты системы безопасности Windows 2000, основанные на шифровании с применением открытого ключа.

Продолжительность занятия — около 35 минут.

Защищенные каналы

В Windows 2000 пакет аутентификации Secure Channel (SChannel) расположен ниже интерфейса Security Support Provider Interface (SSPI) (рис. 11-7).

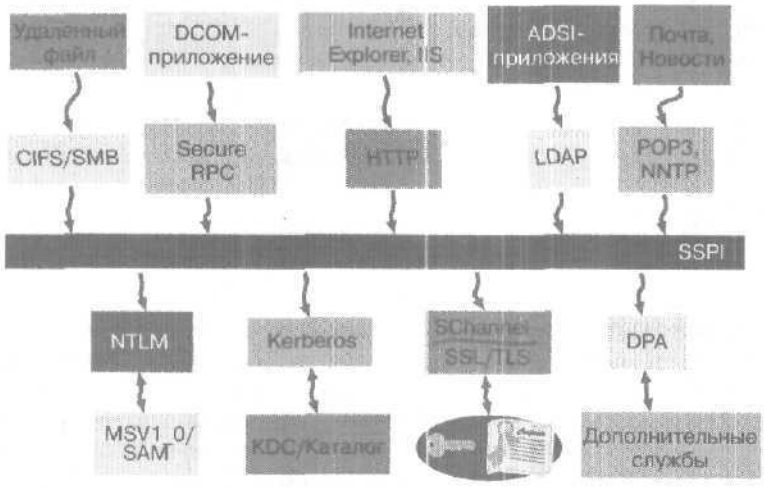


Рис. 11-7. Архитектура Authentication Services в Windows 2000

Пакет аутентификации SChannel поддерживает протоколы Secure Sockets Layer (SSL) 3.0 и Transport Layer Security (TLS) J.O. SSL и TLS — гибкие защищенные протоколы, способные выполняться поверх прочих транспортных протоколов — основаны на технологии аутентификации с применением открытых ключей и для создания уникального ключа шифрования для каждого сеанса связи клиента с сервером обмениваются открытыми ключами.

Протокол TLS основан на протоколе SSL 3.0 и теперь стандартизирован IETF. Хотя различия между TLS 1.0 и SSL 3.0 и незначительны, взаимодействовать TLS 1.0 и SSL 3.0 не могут. Впрочем, в TLS 1.0 предусмотрен механизм согласования, поэтому TLS может использовать SSL 3.0. Следовательно, клиент, поддерживающий только SSL 3.0, может общаться с сервером, поддерживающим TLS 1.0.

И SSL, и TLS, обеспечивают безопасную передачу информации путем шифрования, аутентификации клиента и (необязательно) аутентификации сервера. Оба применяются

для обмена конфиденциальными данными по Интернету с применением аутентификации по открытому ключу.

Протокол SSL/TLS обеспечивается поставщиком SChannel (таким как IIS, Proxy Server и Exchange) и клиентским интернет-приложением (например Internet Explorer или клиент электронной почты Outlook). Приложения запрашивают службы SSL и TLS через API-интерфейс SSPI.

SSL и TLS дают следующие преимущества:

- аутентификация гарантирует клиенту, что данные посылаются на нужный сервер и этот сервер защищен;
- шифрование гарантирует, что данные сможет прочитать только целевой защищенный сервер;
- проверка целостности обеспечивает неизменность полученных данных.

Смарт-карты

Применяются для хранения открытого и закрытого ключа пользователя и сертификата. Это более надежный способ защиты и контроля ключей пользователя, чем хранение их на компьютере. Пользовательские ключи и сертификаты перемещаются вместе с ним. Смарт-карта производит уязвимые с точки зрения безопасности вычисления, не открывая закрытый ключ пользователя компьютеру.

Для работы со смарт-картой компьютеру требуется устройство считывания. Смарт-карта — это совместимое со стандартом ISO 7816 устройство, содержащее встроенный микропроцессор, RSA или эквивалентный криптографический сопроцессор и локальное запоминающее устройство. Локальное запоминающее устройство включает:

- 6–24 кб ПЗУ для ОС смарт-карты и программ;
- 128-512 байт ОЗУ для временных данных;
- 1-16 кб ОЗУ для данных пользователя.

Вход в систему с помощью смарт-карты

Windows 2000 поддерживает вход в систему со смарт-карты как альтернативу паролям для доменной аутентификации. Для этого применяется PC/SC-совместимая инфраструктура смарт-карт, введенная в Windows NT/95 в декабре 1997 т., и RSA-совместимые смарт-карты с поддержкой поставщиков служб криптографии на основе интерфейса Crypto API. Для взаимодействия с системой контроля доступа Kerberos в процессе аутентификации используется протокол PKINIT.

Система распознает событие вставки смарт-карты как альтернативу стандартной комбинации клавиш Ctrl+Alt+Del для входа, а затем запрашивает у пользователя PIN-код смарт-карты, открывающий доступ к операциям с сохраненным на смарт-карте закрытым ключом. Смарт-карта также содержит копию сертификата пользователя (выпущенного ЦС предприятия). Это позволяет пользователю входить в домен с разных компьютеров.

Технология Authenticode

Широкое использование Интернета увеличило зависимость от его активного содержания: Windows-приложений, элементов управления ActiveX и Java-апплетов. Появилась острая необходимость защитить клиентские системы от опасного кода, зачастую выполняемого без ведома пользователя. В 1996 г. Microsoft была введена технология цифровой подписи Authenticode, а в 1997 г. она была значительно усовершенствована.

Технология Authenticode, элемент безопасности в Microsoft Internet Explorer, гарантирует аутентификацию программных компонентов в Интернете. Authenticode проверяет, что ПО не искажено и распознает его изготовителя. В каждом конкретном случае пользователи могут принимать решения о загрузке кода, основанные на их опыте и доверии изготовителю ПО. Подпись, которую разработчики удостоверяют свой код, — основа доверия к ним со стороны пользователей.

Authenticode позволяет разработчикам ПО ставить цифровую подпись на любую форму активного содержания, включая многотомные архивы. Эти подписи могут быть использованы для проверки как разработчиков содержимого, так и целостности самого содержимого при загрузке. Windows 2000 PKI позволяет выпускать Authenticode-сертификаты для внутренних разработчиков или подрядчиков, так что любой сотрудник может проверить источник и целостность загружаемых приложений.

Шифрованная файловая система

Позволяет пользователям шифровать и расшифровывать файлы и применяется для защиты файлов от злоумышленников, которые могут получить несанкционированный физический доступ к хранимым конфиденциальным данным (например, украв переносной компьютер или внешний диск).

Для обеспечения секретности данных в процессе шифрования применяется открытый ключ пользователя. Посторонние не смогут расшифровать информацию без соответствующего закрытого ключа. Для каждого зашифрованного файла создается специальный восстанавливающий ключ — его использует компетентный администратор в экстренных ситуациях, например в случае отсутствия сотрудника или при потере закрытого ключа.

Шифрование/расшифровка производится в ходе ввода-вывода автоматически и практически не влияет на производительность.

EFS также поддерживает шифрование/расшифровку файлов на удаленных томах NTFS. Файлы могут быть экспортированы в зашифрованном виде, но по умолчанию данные перемещаются по сети незашифрованными. Для шифрования данных при перемещении по сети Windows 2000 поддерживает сетевые протоколы SSL, TLS и IPSec.

Защита данных

EFS использует комбинацию открытого и закрытого ключей пользователя, а также выбранный случайным образом *ключ шифрования файла* (file encryption key, FEK). FEK — это 128-разрядный ключ в версии для Северной Америки и 40-разрядный — для международных версий. Windows 2000 использует для шифрования файлов алгоритм Data Encryption Standard X (DESX).

Восстановление данных

Политика восстановления зашифрованных данных (Encrypted Data Recovery Policy, EDRP) указывает, кто может восстановить данные в случае, если личный ключ пользователя утерян. На изолированных компьютерах EDRP генерируется автоматически для упрощения администрирования. Компьютеры домена получают EDRP из политики домена. По соображениям безопасности восстанавливают только зашифрованные данные, а ключи пользователей восстановить нельзя.

Шифрование при резервном копировании и восстановлении

Так как члены группы Backup Operators (Операторы архива) не имеют ключей для расшифровки, шифрованные данные считываются и записываются в резервную копию как фоновый поток данных.

Отказоустойчивость

Шифрование и расшифровка — операции уязвимые, так как сбой может привести к потере данных. Поэтому EFS выполняет все операции автоматически. Операция, которая не может быть завершена, отменяется. Например, если электропитание компьютера отключается при шифровании, EFS отменяет эту операцию при перезагрузке, и файл остается в исходном состоянии.

После того как файл зашифрован, процессы шифрования/расшифровки проходят автоматически и незаметно для пользователей и программ. За раз можно зашифровать один файл или одну папку.

Вы можете зашифровать файл или папку в Windows Explorer или из командной строки.

Примечание Невозможно одновременно использовать сжатие NTFS и шифрование для одного и того же файла — это взаимоисключающие операции.

Шифрование в EFS

EFS шифрует, дешифрует и восстанавливает файлы (рис. 11-8).

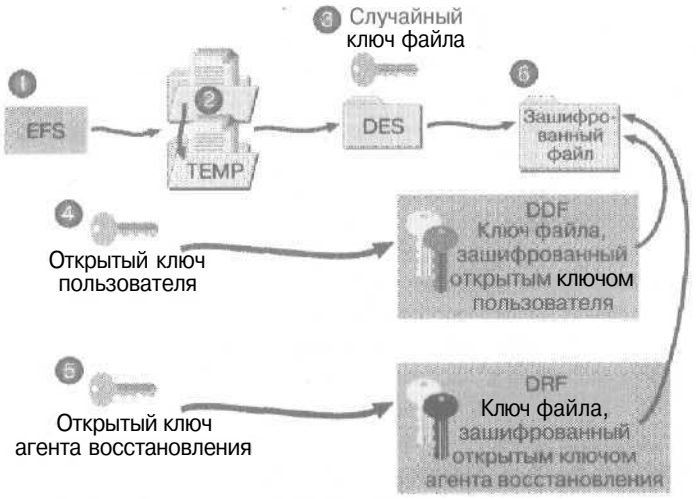


Рис. 11-8. Процесс **шифрования в EFS**

Когда пользователь шифрует файл в EFS, происходит следующее.

1. Служба EFS открывает файл для монопольного доступа.
2. Все данные, записываемые в файл, копируются во временный файл.
3. Ключ файла генерируется случайным образом и используется для шифрования файла согласно схеме шифрования DES.
4. Создается *поле расшифровки данных* (Data Decryption Field, DDF), которое содержит ключ файла, зашифрованный открытым ключом пользователя.
5. Создается *поле восстановления данных* (Data Recovery Field, DRF), содержащее ключ файла, на этот раз зашифрованный открытым ключом агента восстановления. Открытый ключ агента восстановления извлекается из EDRP.
6. Сервер EFS записывает шифрованные данные с DDF и DRF обратно в файл,

Расшифровка в EFS

Процесс расшифровки использует поле DDF, созданное при шифровании (рис, 11-9).

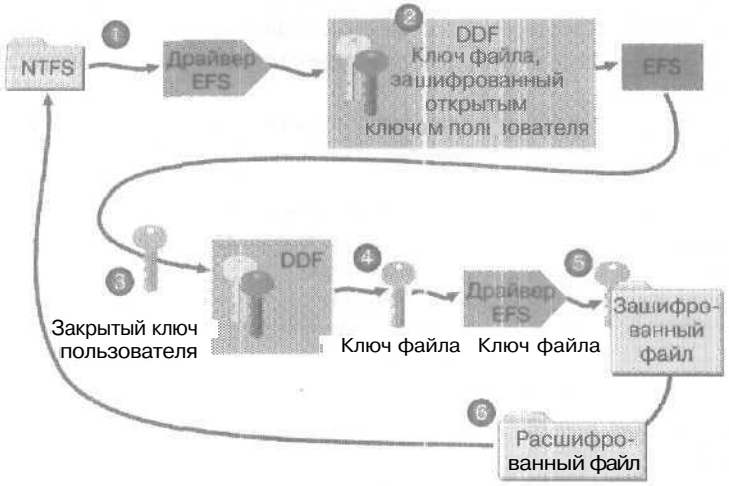


Рис. 11-9. Процесс расшифровки в EFS

Когда файл дешифруется в EFS, происходит следующее.

1. Когда какая-либо программа открывает зашифрованный файл, NTFS посылает запрос драйверу EFS.
2. Драйвер EFS возвращает значение DDF и передает его службе EFS,
3. Служба EFS дешифрует DDF с помощью закрытого ключа пользователя и получает ключ файла.
4. Служба EFS передает ключ файла обратно драйверу EFS.
5. Драйвер EFS использует ключ файла для расшифровки файла.
6. Драйвер EFS возвращает расшифрованные данные файловой системе NTFS, которая завершает запрос файла и посылает данные программе-заказчику.

Восстановление EFS

Восстановление EFS сходно с процессом расшифровки (рис. 11-10).

Когда файл восстанавливается в E.FS, происходят следующие процессы.

1. NTFS посылает запрос драйверу EFS.
2. Драйвер EFS возвращает DRF и передает его службе EFS.
3. Служба EFS восстанавливает DRF, пользуясь закрытым ключом агента восстановления для получения ключа файла.
4. Служба EFS отправляет ключ файла обратно драйверу EFS.
5. Драйвер EFS использует ключ файла для восстановления файла.
6. Драйвер EFS возвращает зашифрованные данные файловой системе NTFS, которая завершает запрос файла и посылает данные программе-заказчику.

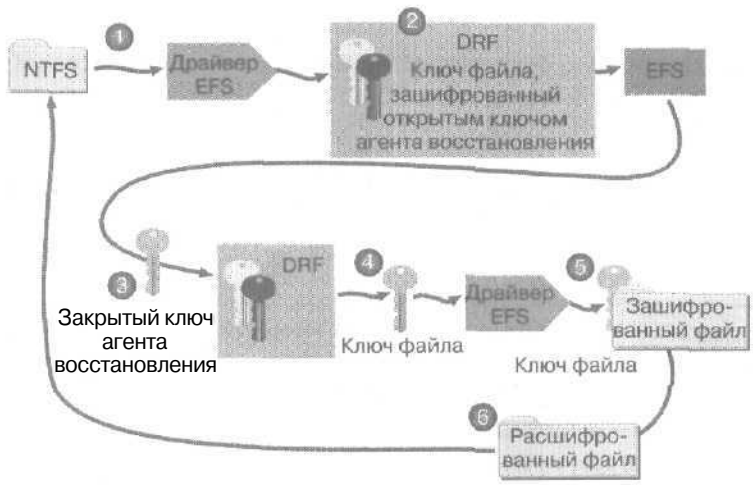


Рис. 11-10. Процесс восстановления EFS

Утилита командной строки cipher

Утилита cipher позволяет шифровать/дешифровать файлы из командной строки:

`cipher [/e /d] [/s:каталог][/a][/i] [/f] [/q] [/h] [/k] [путь [...]]`

Без параметров cipher показывает состояние шифрования текущей папки и файлов внутри ее. Можно использовать несколько имен папок или ввести в имени папки метасимволы. Несколько параметров команды следует разделять пробелами. Параметры cipher таковы.

Параметр	Описание
/e	Зашифровывает указанные папки. Папки маркируются так, что добавленные впоследствии файлы будут также зашифрованы.
/d	Расшифровывает указанные папки. Папки маркируются так, что добавленные впоследствии файлы зашифрованы не будут.
/s:dir	Выполняет выбранную операцию в указанной папке и всех подпапках.
/a	Выполняет операцию как для файлов, так и для каталогов. Рекомендуется шифровать файл и папку, которая его содержит, потому что при изменении зашифрованного файла в незашифрованной папке шифр может быть снят. Если подходящего файла нет, этот параметр игнорируется.
/I	Продолжает выполнение указанной операции даже после обнаружения ошибок. По умолчанию работа cipher останавливается, если встречаются ошибки.
/f	Принудительно шифрует все выбранные объекты, даже если они уже зашифрованы. По умолчанию ранее зашифрованные объекты пропускаются.
/q	Выводит только наиболее важную информацию.
/h	Отображает скрытые или системные файлы. По умолчанию эти файлы пропускаются.
/k	Создает новый ключ шифрования файла для пользователя, запустившего cipher. Остальные выбранные параметры будут проигнорированы.
путь	Определяет шаблон имени, имя файла или имя папки полностью.

Примеры

Чтобы зашифровать папку C:\My Documents, наберите в командной строке **cipher /e «My Documents».** Чтобы зашифровать все файлы на диске C: со словом «test» в имени файла, наберите в командной строке **cipher /e /s *test*.**

Упражнение 2: конфигурирование и использование EFS

Сконфигурируйте политику восстановления данных в домене и зашифруйте папку. Упражнение выполняйте на Server01.

Примечание Для дополнительной практики откройте файл \chapt11\articles\efs-wp.doc на прилагаемом компакт-диске и выполните упражнения 2–7 (начиная со страницы 12).

▶ Задание 1: настройте политику восстановления в домене

Политика восстановления конфигурируются по умолчанию, когда устанавливается первый контроллер домена. В итоге самостоятельно подписанный сертификат назначает агентом восстановления администратора домена. На этом этапе перед использованием EFS вручную добавьте администратора как агента восстановления.

1. Зарегистрируйтесь на ServerOl как Administrator с паролем **password.**
2. В меню Start выберите команду **Run** (Выполнить), в поле Open (Открыть) введите **http://server01/certsrv/** и щелкните кнопку OK.

   В Internet Explorer откроется страница работы с сертификатами.
3. Выберите переключатель Request A Certificate (Запросить сертификат) и щелкните Next (Далее).

   Откроется страница Choose Request Type (Выбор типа запроса).
4. Щелкните переключатель Advanced Request (Расширенный запрос), а затем — кнопку Next (Далее).

   Откроется страница Advanced Certificate Requests (Расширенные запросы на сертификаты).
5. Проверьте, что выбран переключатель Submit A Certificate Request To This CA Using A Form (Выдать запрос на сертификат этому ЦС, используя форму), затем щелкните кнопку Next (Далее).
6. В списке Certificate Template (Шаблон сертификата) выберите EFS Recovery Agent (Агент восстановления EFS).
7. Щелкните кнопку Submit (Выдать запрос).

   Откроется страница Certificate Issued (Сертификат выдан).
8. Щелкните ссылку Install This Certificate (Установить этот сертификат).

   Откроется страница Certificate Installed (Сертификат установлен).
9. Закройте Internet Explorer.
10. **Из** программной группы Administrative Tools (Администрирование) откройте оснастку Active Directory Users And Computers (Active Directory — пользователи и компьютеры).
11. В дереве консоли выберете узел microsoft.com.
12. В меню Action (Действие) выберите команду Properties (Свойства).
13. Откроется диалоговое окно microsoft.com Properties (Свойства: microsoft.com).
14. На вкладке Group Policy (Групповая политика) щелкните кнопку Edit (Изменить).

    Откроется оснастка Group Policy (Групповая политика).

15. Под узлом Computer Configuration (Конфигурация компьютера) раскройте контейнер Windows Settings (Конфигурация Windows), затем узел Security Settings (Параметры безопасности), контейнер Public Key Policies (Политики открытого ключа) и контейнер Encrypted Data Recovery Agents (Агенты восстановления шифрованных данных).
16. В меню Action (Действие) выберите команду Add (Добавить).

    Откроется окно мастера Add Recovery Agent (Мастер добавления атента восстановления).
17. Щелкните кнопку Next (Далее).

    Откроется окно Select Recovery Agents (Выбор агентов восстановления).
18. Щелкните кнопку Browse Directory (Обзор каталога).

    Откроется диалоговое окно Find Users, Contacts and Groups (Поиск: пользователи, контакты и группы).
19. Щелкните кнопку Find Now (Найти).
20. В списке найденных пользователей и групп дважды щелкните Administrator (Администратор).

    Откроется окно Select Recovery Agents (Выбор агентов восстановления).
21. Щелкните кнопку Next (Далее).

    Откроется окно завершения работы мастера,
22. Щелкните кнопку Finish (Готово).

    На правой панели оснастки Group Policy (Групповая политика) появится строка Administrator (Администратор).
23. Щелкните эту строку.
24. В меню Action (Действие) выберите команду Properties (Свойства).

    Откроется диалоговое окно Administrator Properties.

    Заметьте: для этого сертификата в принципе доступны все назначения, а в настоящее время лишь одно — File Recovery (Восстановление файлов).
25. Щелкните кнопку OK.
26. Закройте оснастку Group Policy.

    Откроется диалоговое окно свойств microsoft.com.
27. Щелкните кнопку OK.

    Откроется оснастка Active Directory Users And Computers,
28. В меню View (Вид) выберите команду Advanced Features (Дополнительные функции).
29. В дереве консоли щелкните контейнер Users.
30. На правой панели щелкните Administrator (Администратор).
31. В меню Action (Действие) выберите команду Properties (Свойства).

    Откроется диалоговое окно Administrator Properties (Свойства: Администратор).
32. Щелкните вкладку Published Certificates (Опубликованные сертификаты).

    Появится список сертификатов стандарта X.509, изданных для данной учетной записи пользователя.

    Заметим, что были изданы два сертификата для учетной записи Administrator и от его имени. Сертификат, внесенный в список как File Recovery (Восстановление файлов) в колонке Intended Purpose (Назначение), используют для восстановления зашифрованных файлов с EFS, если оригинальный закрытый ключ потерян или недействителен по иной причине.
33. Щелкните кнопку OK.
34. Закройте оснастку Active Directory Users And Computers.

► **Задание 2: зашифруйте папку с использованием EFS**

Зашифруйте папку на Server01 с помощью Windows Explorer.

1. На рабочем столе дважды щелкните ярлык My Computer (Мой компьютер).
2. Дважды щелкните диск Local Disk (C:) [Локальный диск (C:)].
3. Дважды щелкните папку Document And Settings.
4. Дважды щелкните папку Administrator (Администратор).
5. Выделите папку My Documents (Мои документы).
6. В меню File (Файл) выберите команду Properties (Свойства).
   Откроется диалоговое окно My Documents Properties (Свойства: Мои документы).
7. Щелкните кнопку Advanced (Другие).
   Откроется диалоговое окно Advanced Attributes (Дополнительные атрибуты).
8. Пометьте флажок Encrypt Contents To Secure Data (Шифровать содержимое для защиты данных) и дважды щелкните кнопку OK, чтобы закрыть окно свойств папки,
9. Закройте окно Administrator.

Протокол IPSec

В предыдущей главе, обсуждая протоколы передачи данных, мы кратко рассмотрели IPSec. В этой главе мы подробно расскажем, как IPSec применяется с открытым ключом. IPSec в Windows 2000 предназначен для защиты особо уязвимых данных в сети TCP/IP и обеспечивает конфиденциальность, целостность и аутентификацию трафика IP для каждого пакета.

При использовании IPSec два связывающихся компьютера сначала согласовывают наиболее строгие общие политики безопасности, а затем каждый на своей стороне управляет IP Security. Перед отправкой данных компьютер, инициализируя связь, прозрачно для пользователя зашифровывает данные с помощью IP Security. Принимающий компьютер так же прозрачно расшифровывает данные перед передачей их принимающему процессу. Поскольку данные передаются на уровень протокола IP и там зашифровываются, отдельные защищенные пакеты для каждого протокола в наборе TCP/IP не требуются.

Использование IPSec для шифрования всего IP-трафика сети гарантирует, что любая связь, основанная на TCP/IP, защищена от перехвата. Любые маршрутизаторы между связывающимися компьютерами могут просто перенаправлять зашифрованные пакеты IP.

Примечание Для гарантии полной совместимости с предыдущими версиями Windows компьютер с Windows 2000, сконфигурированный под IPSec, посылает данные на компьютеры, работающие с предыдущими версиями Windows без шифрования.

Политики IPSec

С Windows 2000 IPSec Вы можете создавать политики, определяющие тип и уровень безопасности в сети.

Политики согласования

Определяют используемые в сети службы безопасности. Протокол безопасности, выбранный для этих политик согласования, является основой для служб безопасности. Например, если выбран протокол IP Authentication Header, обеспечивается целостность, аутентификация и предотвращение повтора, но не конфиденциальность.

Вы можете задать несколько способов обеспечения безопасности для каждой политики согласования. Если первый способ неприемлем для безопасного соединения, служба продолжит поиск в списке, пока не найдет политику, пригодную для установления связи. Если согласование не удалось, связь устанавливается без IPSec.

Фильтры IP

Руководят действиями в зависимости от пункта назначения пакета IP, активного IP-протокола и используемых портов. Каждый IP-пакет проверяется IP-фильтром, и если соответствие найдено, то для посылки сообщения применяется соответствующая политика безопасности. Фильтры должны быть сконфигурированы как для входящего, так и для исходящего трафика.

Политики безопасности

Используют для конфигурирования атрибутов IPSec. Они создаются соответствующими политиками согласования и фильтрами IP и связаны с политиками контроллера домена. Политики безопасности определяют тип и уровень безопасности для любого сетевого IP соединения. Политики безопасности IP могут быть назначены в качестве политики домена по умолчанию, локальной политики по умолчанию или политики домена по выбору.

Подключающийся к домену компьютер автоматически получает политики домена и локальные политики по умолчанию, в том числе политику IPSec для домена.

Компоненты IPSec

Процедура установки Windows 2000 устанавливает службы, протоколы и драйверы для IPSec:

- службу IPSec Policy Agent;
- Internet Security Association и протокол Key Management Protocol (ISAKMP);
- протокол Oakley Key Management;
- драйвер IPSec.

Протоколы ISAKMP и Oakley Key Management обычно называют протоколами ISAKMP/Oakley (IKE).

Служба IPSec Policy Agent

В момент инициализации системы IPSec Policy Agent извлекает правила IPSec из Active Directory. IPSec Policy Agent передает эти сведения сетевому драйверу IPSec и протоколам IKE. IPSec Policy Agent не сохраняет правила на локальных носителях; вместо этого они извлекаются из хранилища Active Directory. IPSec Policy Agent запускает как протоколы IKE, так и драйвер IPSec.

Протоколы IKE

Протоколы ISAKMP/Oakley (IKE) проводят согласование и устанавливают между компьютерами сопоставление безопасности связь (Security Association, SA). Служба Kerberos аутентифицирует связывающиеся компьютеры. Наконец, протоколы ISAKMP/Oakley (IKE) посылают драйверу IPSec сведения о ключе и SA.

Драйвер IPSec

Проверяет все пакеты IP на соответствие фильтру IP. Если соответствие найдено, драйвер IPSec удерживает пакеты в очереди, пока протоколы IKE генерируют необходимое SA и ключ для зашифровки пакета. Получив информацию от протоколов IKE, драйвер IPSec шифрует IP-пакеты и посылает их на принимающий компьютер.

Пример связи по IPSec

В этом примере пользователь User 1 на Computer A посылает данные пользователю User 2 на Computer B. IP Security применяется на обоих компьютерах (рис. 11-11).

На уровне пользователя обеспечение безопасности IP-пакетов не видно и осуществляется следующим образом.

1. User 1 запускает программу, которая соединяется по сети, используя TCP/IP для пересылки данных User 2. Политики безопасности, установленные на Computer A и Computer B определяют уровень безопасности сетевой связи.
2. Служба IPSec Policy Agent получает политики и передает их протоколам ISAKMP/Oakley и драйверу IPSec.
3. Протоколы ISAKMP/Oakley на каждом компьютере используют политики согласования, соответствующие установленной политике SA. Результаты согласования передаются между двумя компьютерами на драйвер IPSec, использующий полученный ключ для шифрования данных.
4. Наконец, драйвер IPSec посылает зашифрованные данные на Computer B. Драйвер IPSec на Computer B расшифровывает данные и пересылает их принимающей программе.

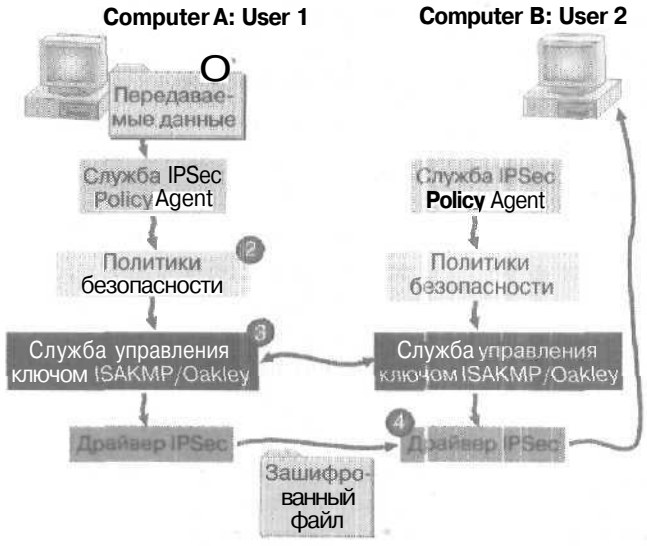


Рис. 11-11. Пример процесса связи с применением IPSec

Резюме

Windows 2000 поддерживает цифровые технологии, основанные на шифровании открытым ключом: пакет аутентификации SChannel, смарт-карты, Authenticode, шифрованную файловую систему (EFS) и защиту IPSec. Пакет SChannel управляет SSL 3.0 и TLS 1.0 — настраиваемыми протоколами безопасности, выполняющимися поверх других транспортных протоколов. Смарт-карты могут хранить открытый и закрытый ключи пользователя и сертификат. Это более надежный способ для зашиты и работы с ключами пользователя, чем хранение их на компьютере. Технология Authenticode позволяет издателям ПО заверять цифровой подписью любые формы активного содержания, включая многотомные архивы. Эти подписи могут быть использованы для проверки как издателей содержимого, так и сохранности содержимого при загрузке. EFS — это расширение для файловой системы NTFS, обеспечивающее усиленную защиту данных и шифрование для файлов и папок. Технология шифрования, основанная на применении открытых ключей, работает как интегрированная системная служба. Протокол IPSec, встроенный в Windows 2000 для защиты особо уязвимых данных в сети TCP/IP, обеспечивает конфиденциальность, целостность и аутентификацию каждого пакета IP-трафика.

Занятие 3. Протокол Kerberos в Windows 2000

Стандартный процесс обеспечения безопасности означает включение в систему функции, заставляющей пользователя доказывать, что он именно тот, за кого себя выдает. Эта проверка подлинности выполняется, когда пользователь вводит правильный пароль для данной учетной записи. Например, когда User 1 пытается соединиться с некоторым сервером для доступа к какому-либо файлу, этот сервер должен убедится, что посылает запрос действительно User 1. Обычно сервер предполагает, что это User 1, если при установлении связи вводится правильный пароль. Более надежный вариант обеспечивается доверенной третьей стороной, проверяющей идентичность пользователя. Такой стороной является протокол аутентификации Kerberos.

Изучив материал этого занятия, Вы сможете:

- ✓ описать протокол Kerberos и его работу в Windows 2000.

Продолжительность занятия — около 35 минут.

Обзор протокола Kerberos

В Windows 2000 протокол Kerberos является службой аутентификации по умолчанию и основным протоколом безопасности. Он позволяет пользователю получить доступ ко всем ресурсам сети после однократной регистрации. Kerberos проверяет как подлинность пользователя, так и целостность данных во время сеанса связи. Это обусловлено тем, что служба Kerberos устанавливается на каждом контроллере домена, а клиент Kerberos — на все компьютеры с Windows 2000.

Примечание Клиент Active Directory для Windows 9x позволяет пользователю входить я систему по протоколу аутентификации Kerberos V5.

При наличии протокола аутентификации Kerberos служба Kerberos на сервере проверяет подлинность пользователя. Прежде чем связаться с сервером, пользователь запрашивает билет от службы Kerberos — *центра распространения ключей* (Key Distribution Center, KDC) — для подтверждения своей личности. Затем пользователь посылает этот билет на целевой сервер. Так как сервер доверяет Kerberos, ручающейся за личность пользователя, он принимает пропуск как доказательство подлинности пользователя.

Протокол Kerberos не дает пользователям входить в систему и получать доступ к ресурсам простым введением правильного имени и пароля. Вместо того чтобы верить введенным данным, ресурс должен войти в контакт со службой Kerberos и получить пропуск, удостоверяющий пользователя. Kerberos выступает как доверяемая третья сторона, генерирующая сеансовый ключ и предоставляющая пропуск для данной сессии клиент-сервер.

Выпускаемый службой Kerberos билет включает:

- сеансовый ключ;
- имя пользователя, для которого выдан сеансовый ключ;
- срок действия билета;
- любые дополнительные требуемые поля данных или параметры.

Срок действия билета определяется системными правилами домена. Если срок действия билета кончился во время сеанса, служба Kerberos извещает клиента и сервер о необходимости восстановления билета. Затем Kerberos генерирует новый сеансовый ключ, и сеанс продолжается.

Термины протокола Kerberos

Чтобы лучше понять протокол Kerberos, Вы должны ознакомиться с его терминологией.

Участник безопасности

Участник безопасности (principal) — это имеющий уникальное имя пользователь, клиент или сервер, участвующий в сеансе связи.

Сфера

Сфера (realm) — это граница аутентификации, которую можно сравнить с доменом Windows 2000. Каждая организация, использующая сервер Kerberos, создает собственную сферу. Домен Windows 2000 — это на самом деле сфера Kerberos, она называется доменом только для совместимости с терминологией Windows NT.

Секретный ключ

Используется совместно клиентом или сервером и третьей стороной для шифрования передаваемой между ними информации. В случае Kerberos доверяемой третьей стороной является служба Kerberos. В случае участника безопасности секретный ключ обычно основан на случайных данных или шифровании паролем участника. Секретный ключ никогда не передается по сети; передается только зашифрованная информация.

Сеансовый ключ

Этот временный ключ шифрования используется двумя участниками безопасности ограниченное время в течение единственного сетевого соединения. Связывающиеся партнеры обмениваются сеансовым ключом, поэтому он называется общим секретом. Сеансовый ключ всегда посылают в зашифрованном виде.

Аутентификатор

Это запись, используемая для проверки того, что запрос действительно исходит от данного участника безопасности. Аутентификатор содержит информацию, проверяющую идентичность отправителя и время посылки запроса. Эта информация зашифрована с помощью общего сеансового ключа, известного только связывающимся участникам безопасности. Аутентификатор обычно посылают с билетом, чтобы дать возможность получателю удостовериться, что именно данный клиент инициализировал запрос.

Центр распространения ключей

Выполняет две роли: *сервера аутентификации* (authentication server, AS) и *службы предоставления билета* (ticket granting service, TGS). TGS рассылает билеты клиентам, подключающимся к сетевым службам. Но прежде чем клиент воспользуется службой TGS для получения билета, он должен получить *специальный билет для получения билета* (ticket granting ticket, TGT) от AS.

Сертификат атрибута привилегий

Сертификат атрибута привилегий (privilege attribute certificate, PAC) содержит *идентификатор безопасности* (security ID, SID) пользователя.

Билет

Клиент связывается с TGS и запрашивает билет для сервера, с которым он соединяется, до контакта с ним. *Билет* (ticket) — это запись, позволяющая клиенту аутентифицировать себя для сервера; этот просто сертификат, выдаваемый службой Kerberos. Билет зашифрован так, что только сервер-адресат способен расшифровать и прочитать его. Билет содержит идентификационные данные клиента-заказчика, штамп времени, сеансовый ключ серверов, срок годности билета, а также другие данные (вроде PAC) для идентификации клиента целевым сервером. Билет пригоден для многократного пользования, его срок службы обычно составляет 8 часов.

Билет на получение билета

Один из способов применения Kerberos состоит в том, чтобы просто запрашивать билет на каждый целевой сервер у TGS всякий раз, когда пользователь хочет получить доступ на определенный сервер. Ответ на запрос в этом случае может содержать сеансовый ключ и другие сведения, зашифрованные секретным ключом пользователя. Этот способ приводит к открытости составной части секретного ключа пользователя в сети при запросе на создание нового билета.

В Windows 2000 Kerberos защищает секретный ключ тем, что сначала аутентифицирует пользователя, а затем запрашивает билет для получения билета (TGT). *Билет для получения билета* — это запрос билета и выбранного случайным образом сеансового ключа для применения совместно с компонентом TGS службы Kerberos, Получив билет, пользователь может контактировать со службой в любое время; билет приходит не от TGS, а от AS. Чтобы задействовать TGS, ответ зашифровывается не секретным ключом пользователя, а сеансовым ключом, полученным от **AS.**

Возможности протокола Kerberos

У Kerberos есть несколько преимуществ перед традиционной системой аутентификации запрос-ответ.

Полностью открытый стандарт

Реализация протокола Kerberos в Windows 2000 со стандартами RFC 1510 и RFC 1964. Она может взаимодействовать с другими реализациями Kerberos, также совместимыми с RFC. Поэтому клиенты Kerberos, использующие другие платформы, такие как UNIX, могут быть аутентифицированы Windows 2000. Иногда, однако, данных, зависящих от реализации, может не быть или они недоступны. При отсутствии нужных данных служба Kerberos в Windows 2000 пытается найти имя участника безопасности из билета в списке учетных записей Windows 2000 или в создаваемой по умолчанию для этих целей учетной записи.

Ускоренная аутентификация при подключении

Серверам не нужно выполнять сквозную аутентификацию. Сервер Windows 2000 может проверять личность клиента по его билету без запроса к службе Kerberos. Это возможно потому, что клиент уже получил билет Kerberos от контролера домена, и сервер может использовать его для построения маркера доступа клиента. Выполняя меньше работы при установлении соединения, сервер может обработать большее число одновременно поступающих запросов.

Взаимная аутентификация

Kerberos обеспечивает взаимную аутентификацию клиента и сервера. Протокол аутентификации NTLM в Windows обеспечивает аутентификацию только клиента, предполагая, что все серверы надежны. Он не проверяет подлинность сервера, с которым связывается клиент. Но предположение, что все серверы надежны, не вполне обосновано. Взаимная аутентификация клиента и сервера, безусловно, нужна.

Делегирование аутентификации

Позволяет пользователю подключаться к серверу приложения, который в свою очередь может подключаться к одному или более серверам от имени клиента по удостоверению личности клиента.

Транзитивные доверительные отношения

Удостоверение личности, выданное одной службой Kerberos, действительно для всех служб Kerberos внутри домена.

Процесс аутентификации с помощью Kerberos

Заключается в согласующих обменах между клиентом и целевым сервером, а также между клиентом и KDC (рис. 11-12).

Рис. 11-12. Процесс аутентификации с помощью Kerberos

Процесс аутентификации с помощью Kerberos выполняется следующим образом.

1. Пользователь посылает начальный AS-запрос компоненту AS службы Kerberos. AS содержит основное имя клиента и основное имя сервера, для которого запрашивается билет.
2. Служба Kerberos генерирует AS-ответ и посылает его клиенту.

   Ответ содержит:

   - TGT для компонента TGS службы Kerberos; TGT зашифровывается секретным ключом TGS и содержит SID пользователя; при этом клиент неспособен изменить данные SID;
   - сеансовый ключ для обмена с компонентом TGS службы Kerberos; этот ключ шифруется закрытым ключом пользователя; последний вычисляется по паролю клиента и сходен с сеансовым ключом, используемым в системе NTLM; это затрудняет взлом сеансового ключа.
3. Клиент генерирует и посылает TGS-запрос, содержащий основные имена клиента и соединяемого сервера, а также TGT, идентифицирующий клиента.
4. Компонент TGS службы Kerberos генерирует и посылает клиенту TGS-ответ с билетом для соединяемого сервера. Билет шифруется секретным ключом сервера, который вычисляется по паролю, создаваемому при включении сервера в домен. Ответ содержит и другие данные, в частности, сеансовый ключ.
5. Клиент извлекает сеансовый ключ для соединяемого сервера и генерирует для этого сервера запрос, содержащий имя соединяемого сервера и аутентификатор, зашифрованный сеансовым ключом. Клиент посылает этот запрос серверу по установленному способу передачи.
6. Сервер расшифровывает билет, используя свой секретный ключ для получения сеансового ключа. Затем сервер с помощью сеансового ключа расшифровывает аутентификатор, удостоверяющий личность клиента. Если клиент запросил взаимную аутентификацию, сервер генерирует ответ, зашифрованный сеансовым ключом, и посылает

его клиенту. Взаимная аутентификация не только аутентифицирует клиента для сервера, но и сервер для клиента.

Примечание Обмены AS и TGS со службой Kerberos происходят по протоколу UDP через порт 88. Обмены между клиентом и сервером зависят от протокола, используемого этими двумя участниками безопасности.

Делегирование в Kerberos

Иногда серверу приложения требуется соединиться с другим сервером от имени клиента, Как и олицетворение, делегирование позволяет обеспечить надлежащие права доступа, следующие из запроса сервера приложения.

Kerberos поддерживает делегированную аутентификацию. Этот тип аутентификации применяется, когда клиент обращается к нескольким серверам. При этом каждый сервер получает свой билет и аутентифицирует билет запрашиваемого сервера от имени клиента. Ограничений на длину цепочки серверов, делегирующих аутентификацию, не накладывается. В этом отличие от *олицетворения*, при котором сервер получает доступ к удаленным ресурсам со стороны клиента (рис. 11-13).

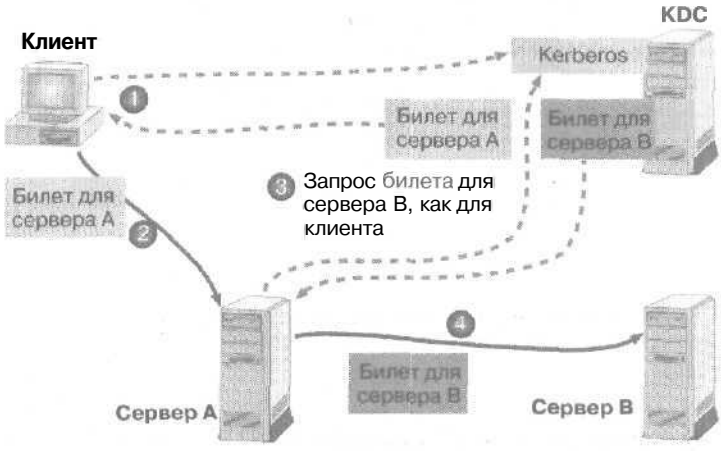


Рис. 11-13. Процесс делегирования в Kerberos

Доступ к ресурсам с участием двух серверов осуществляется следующим образом.

1. Клиент запрашивает и получает билет для сервера А от службы Kerberos.
2. Клиент посылает билет на сервер А.
3. Сервер А посылает запрос, олицетворяя клиента, на службу Kerberos для получения билета для сервера В. Служба Kerberos высылает для клиента билет на сервер В.
4. Затем сервер А посылает этот билет серверу В, получая к нему доступ в качестве клиента.

Вход в систему с помощью Kerberos

Включение Kerberos в Windows 2000 в качестве аутентификационного пакета влияет на многие аспекты процессов входа в систему. Однако некоторые части этих процессов, инициируемые до отправления пакета, остаются неизменными.

Локальный интерактивный вход в систему

При локальном интерактивном входе в систему пользователь подключается по учетной записи с локального компьютера, а не по учетной записи домена (рис. 11-14).

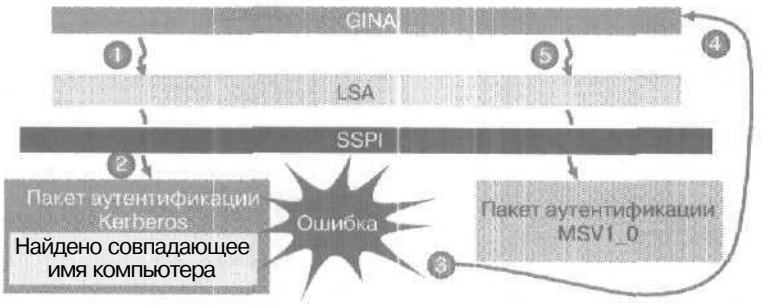


Рис. 11-14. Локальный интерактивный вход в систему

При использовании локальной учетной записи в Windows 2000 происходит следующее.

1. Получив запрос на вход в систему, модуль идентификации Graphical Identification and Authentication DLL (GINA) передает его службе Local Service Authority (LSA). Kerberos в запросе указывается как аутентификационный пакет, так как в Windows 2000 он является таковым по умолчанию.
2. LSA обрабатывает запрос и посылает его Kerberos.
3. В ответ на этот запрос Kerberos возвращает сообщение об ошибке, поскольку он предназначен для аутентификации не локальных, а доменных учетных записей.
4. LSA получает это сообщение об ошибке и возвращает его GINA.
5. GINA повторно посылает запрос LSA с указанием «MSV1_0» в качестве аутентификационного пакета. Затем процесс входа в систему происходит так же, как в Windows NT 4.0.

Интерактивный вход в домен

Обмены при входе в Windows 2000 пользователя с доменной учетной записью похожи на стандартные обмены в Kerberos (рис. 11-15).

Рис. 11-15. Интерактивный вход в домен

Вход в домен осуществляется следующим образом.

1. Получив запрос на вход в систему, LSA передает его Kerberos. Клиент посылает исходный AS-запрос службе Kerberos, сообщая ей имя пользователя и имя домена. Это служит запросом на аутентификацию и TGT. Запрос осуществляется с применением основного имени krbtgt@<*имя_домена*>, где <*имя_домена*> — это имя домена, которому принадлежит учетная запись пользователя. Первый контроллер домена автоматически создает учетную запись krbtgt@<*имя_домена*>.
2. Служба Kerberos генерирует AS-ответ, содержащий TGT (зашифрованный секретным ключом Kerberos) и сеансовый ключ для обменов TGS (зашифрованный секретным ключом клиента) и отсылает его клиенту. Данные авторизации в составе TGT включают SID для учетной записи пользователя и SID для всех групп, к которым он принадлежит. Эти SID возвращаются на LSA для включения в круг доступа пользователя. Kerberos копирует их из TGT в соответствующие билеты, получаемые от этой службы.
3. Затем клиент генерирует и посылает запрос TGS, содержащий основное имя клиента и сферу, TGT для идентификации клиента и имя локальной рабочей станции в качестве сервера. Это делается для запроса доступа пользователя на локальный компьютер.
4. Служба Kerberos генерирует и посылает ответ TGS. Он содержит билет на рабочую станцию и другую информацию, в частности сеансовый ключ (зашифрованный сеансовым ключом с TGT). В данные авторизации включаются S1D для учетной записи пользователя и всех глобальных групп, скопированные службой Kerberos с оригинального TGT.
5. Пакет аутентификации Kerberos возвращает список SID на LSA.

Для аутентификации службы Windows 2000 используют интерфейс SSPI режима ядра. Вместо соединения с Kerberos напрямую обе службы получают доступ к нему через аутентификационный пакет согласования встроенный в LSA (Negotiate package).

При загрузке системы службы Server и Workstation, инициализируют их интерфейс с пакетом согласования в LSA с помощью SSPI. При этом служба сервера получает идентификационные описатели для билетов по умолчанию.

Сетевое соединение устанавливается в два этапа: согласование протокола и настройка сеанса. Прежде чем пользователь установит сеанс связи с сервером, компьютер клиента и сервер должны определить протокол безопасности, исходя из установленного на них уровня безопасности. После того как клиент аутентифицирован и получил билет, он может установить сеанс связи с сервером.

Поддержка открытого ключа в **Kerberos**

Windows 2000 расширяет функциональность Kerberos и разрешает Kerberos взаимодействовать со службой Active Directory. Windows 2000 содержит расширения для протокола аутентификации Kerberos V5, чтобы поддерживать аутентификацию, основанную на открытом ключе. Открытый ключ позволяет клиентам запрашивать исходный TGT, применяя закрытый ключ. Kerberos проверяет этот запрос с помощью открытого ключа пользователя, извлекаемого из сертификата пользователя X.509, находящегося в хранилище Active Directory. Для получения билета сертификат пользователя X.509 должен быть сохранен в соответствующем объекте User. Найдя такой сертификат, Kerberos выдает билет для клиента, и осуществляется стандартная процедура Kerberos. Это заменяет применение секретного ключа, известного только участнику безопасности и KDC. Смарт-карты, например, используют расширения открытого ключа, предоставляемые Kerberos,

Резюме

В Windows 2000 Kerberos является службой аутентификации по умолчанию и основным протоколом безопасности. Чтобы лучше понять протокол Kerberos, надо знать термины Kerberos: участник безопасности, сфера, секретный ключ, сеансовый ключ, аутентификатор, KDC, AS, TGS, PAC, билет и TGT. Процесс аутентификации Kerberos включает согласование компьютера клиента с сервером и KDC. Протокол аутентификации Kerberos поддерживает делегированную аутентификацию. При локальном интерактивном входе в систему пользователь применяет учетную запись, находящуюся на локальном компьютере, а не доменную учетную запись. Обмен, происходящий при входе пользователя в Windows 2000 с доменной учетной записью, похож на обычный обмен Kerberos. Службы Windows 2000 используют для аутентификации интерфейс SSPI режима ядра. Windows 2000 позволяет Kerberos взаимодействовать со службой Active Directory. Windows 2000 содержит расширения протокола Kerberos V5 для поддержки аутентификации, основанной на открытом ключе.

Занятие 4. Средства конфигурации системы безопасности

Windows 2000 включает набор средств конфигурации системы безопасности, предназначенных для облегчения формирования этой системы и анализа состояния сети Windows 2000. Эти инструменты — оснастки MMC, которые позволяют настраивать параметры безопасности Windows 2000 и выполнять периодический анализ этой системы, чтобы убедиться в сохранности параметров настройки или сделать нужные изменения. Параметры безопасности включают в себя политики безопасности (учетная запись и локальные политики), управление доступом (службы, файлы и реестр), журнал регистрации, принадлежность к группе (ограниченные группы), политики безопасности IPSec и открытого ключа. Для конфигурации системы безопасности применяются оснастки Security Configuration And Analysis (Анализ и настройка безопасности), Security Templates (Шаблоны безопасности) и Group Policy (Групповая политика).

Изучив материал этого занятия, Вы сможете:

- ✓ использовать средства конфигурации безопасности и анализировать безопасность систем в сети Windows 2000.

Продолжительность занятия — около 30 минут.

Оснастка Security Configuration And Analysis

Позволяет настраивать и анализировать безопасность локальной системы.

Настройка системы безопасности

Оснастку Security Configuration And Analysis (Анализ и настройка безопасности) можно использовать для прямой настройки безопасности локальной системы. Вы можете импортировать шаблоны безопасности, созданные с помощью оснастки Security Templates (Шаблоны безопасности), и использовать эти шаблоны для *объекта групповой политики* (group policy object, GPO) для локального компьютера. Это позволяет сразу же задать параметры безопасности системы с определенными в шаблоне уровнями.

Анализ безопасности

Состояние ОС и программ на компьютере постоянно меняется. Например, может понадобиться временно изменить уровни безопасности, чтобы решить ряд проблем; эти изменения зачастую могут и далее оставаться в силе. Это значит, что компьютер может перестать удовлетворять требованиям системы безопасности предприятия.

Регулярный анализ позволяет администратору следить за состоянием безопасности и поддерживать должный уровень на каждом компьютере в рамках предприятия. Анализ является всеобъемлющим; его результат содержит сведения обо всех системных аспектах, связанных с безопасностью. Администратор, таким образом, может настраивать уровни безопасности и, что важнее, находить все повреждения системы безопасности, которые время от времени могут иметь место.

Оснастка Security Configuration And Analysis позволяет просмотреть результаты анализа безопасности. Кроме отображения текущих системных параметров, она выдает свои рекомендации, используя значки и метки для указания областей, в которых текущие зна-

чения не соответствуют заданному уровню безопасности. Security Configuration And Analysis также позволяет устранять такие расхождения, обнаруженные в ходе анализа.

Если необходим постоянный анализ большого количества компьютеров, например, в инфраструктуре, основанной на доменах, в качестве средства анализа можно задействовать утилиту командной строки Secedit. Результаты анализа и в этом случае поможет просмотреть оснастка Security Configuration And Analysis. Подробнее об утилите Secedit — в справочной системе Windows 2000.

Оснастка Security Configuration And Analysis

Просматривает и анализирует параметры безопасности системы и выдает рекомендации по их изменению (рис. 11-16). Администратор может задействовать ее для настройки политики безопасности и обнаружения всевозможных брешей.

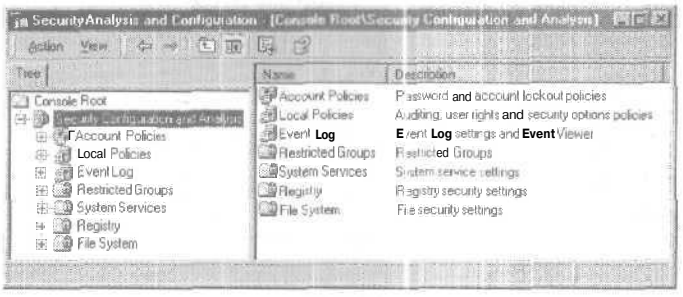


Рис. 11-16. Оснастка Security Configuration And Analysis (Анализ и настройка безопасности)

Оснастка Security Configuration And Analysis позволяет:

- устанавливать рабочую базу данных;
- импортировать шаблон безопасности;
- анализировать безопасность системы;
- просматривать результаты анализа безопасности;
- настраивать безопасность системы;
- изменять базовую конфигурацию безопасности;
- экспортировать шаблон безопасности.

Подробно о выполнении этих задач см. справочную систему Windows 2000.

Оснастка Security Templates

Шаблон безопасности — это физическое представление параметров системы безопасности, т. е. это файл, куда может быть записана группа параметров безопасности. Windows 2000 содержит набор шаблонов безопасности, каждый из которых основан на определенной роли компьютера. Эти шаблоны предусматривают все случаи: от клиентов домена с низким уровнем безопасности до сильно защищенных контроллеров домена. Их можно использовать в исходном виде, модифицировать или сделать основой для создания шаблонов безопасности по выбору пользователя.

Оснастка Security Templates (рис. 11-17) — это инструмент для создания шаблонов и их назначения для одного или нескольких компьютеров.

Шаблон безопасности можно применить на локальном компьютере или импортировать в объект групповой политики в Active Directory. Когда Вы импортируете шаблон безопасности в GPO, групповая политика обрабатывает его и вносит соответствующие изменения для членов GPO — пользователей или компьютеров.

Оснастка Security Templates позволяет:

- выбирать заранее определенный шаблон безопасности;
- задать шаблон безопасности;
- удалять шаблон безопасности;
- обновлять список шаблонов безопасности;
- задать описание для шаблона безопасности.

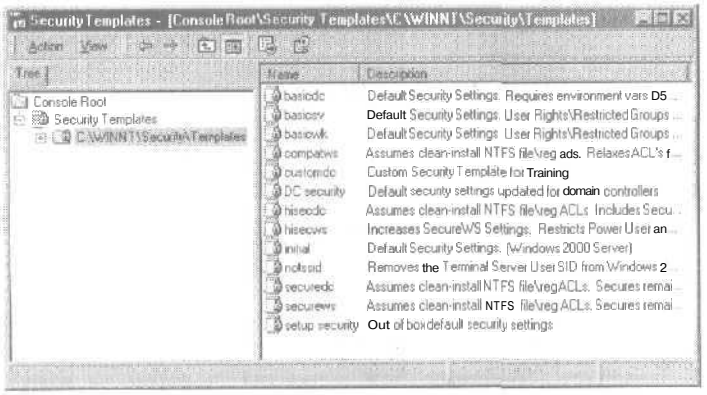


Рис. 11-17. Оснастка Security Templates (Шаблоны безопасности)

Упражнение 3: создание и использование оснастки Security Analysis And Configuration

Создайте собственную оснастку, содержащую оснастки Security Analysis And Configuration (Анализ и настройка безопасности) и Security Templates (Шаблоны безопасности). Затем создайте шаблон и, используя его, откройте новую БД. Проанализируйте параметры безопасности Server01 на соответствие шаблону и примените свой шаблон для задания параметров безопасности на ServerOl. Выполняйте это упражнение на ServerOl.

► Задание 1: создайте консоль для анализа безопасности

Запустите консоль управления MMC и добавьте к ней оснастку Security Analysis And Configuration. Версия 1.2 консоли MMC из состава Windows 2000 позволяет добавлять к ней свои оснастки. Вместо добавления оснасток к существующей консоли создайте новую.

1. Зарегистрируйтесь на ServerOl как Administrator с паролем **password.**
2. В меню Start (Пуск) выберите команду Run (Выполнить).
   Откроется диалоговое окно Run (Запуск программы).
3. В поле Open (Открыть) введите **mmc** и щелкните кнопку OK.
   Откроется пустая консоль MMC с именем Console1 (Консоль1).
4. В меню Console (Консоль) выберите команду Add/Remove Snap-in.
   Откроется одноименное диалоговое окно.
5. Щелкните кнопку Add (Добавить).
   Откроется диалоговое окно Add Standalone Snap-in (Добавить изолированную оснастку).
6. Выберите в списке оснастку Security Configuration And Analysis (Анализ и настройка безопасности) и щелкните кнопку Add (Добавить).
7. Щелкните кнопку Close (Закрыть).

8. Щелкните кнопку OK.
9. В меню Console (Консоль) выберите команду Save (Сохранить).
   Откроется диалоговое окно Save As (Сохранить как).
10. В поле File Name (Имя файла) введите **Security** и щелкните кнопку Save (Сохранить).

► **Задание 2: добавьте и задайте параметры безопасности с помощью оснастки Security Template в консоли Security**

До проведения анализа Server01 и задания новых параметров безопасности установите модуль Security Template в Вашу консоль Security.

1. В меню Console выберите команду Add/Remove Snap-in.
   Откроется диалоговое окно Add/Remove Snap-in.
2. Щелкните кнопку Add (Добавить).
   Откроется окно Add Standalone Snap-in.
3. Выберите в списке оснасток Security Templates (Шаблоны безопасности) и щелкните кнопку Add.
4. Щелкните кнопку Close.
5. Щелкните OK.
6. В меню Console (Консоль) выберите команду Save (Сохранить).
7. Раскройте узел Security Templates (Шаблоны безопасности), а затем -- папку C:\WINNT\Security\Templates.
   Все установленные шаблоны отображаются в дереве консоли и в правой панели.
8. Раскройте узел securedc.
   Этот шаблон более строгой безопасности обычно используется после применения основного шаблона безопасности.
9. Раскройте узел Account Policies (Политики учетных записей) и щелкните папку Password Policy (Политика паролей).
   Параметры политики паролей появятся в правой панели.
10. На правой панели дважды щелкните параметр Minimum Password Length (Мин. длина пароля).
    Откроется диалоговое окно Template Security Policy Setting (Параметр шаблона политики безопасности).
11. В поле Password Must Be At Least (Длина пароля не менее) введите 5 и щелкните кнопку OK.
12. В дереве консоли щелкните пункт securedc.
13. В меню Action (Действие) выберите команду Save As (Сохранить как).
    Откроется одноименное окно.
14. В поле File Name (Имя файла) наберите **customdc** и щелкните кнопку Save (Сохранить).
15. В дереве консоли щелкните пункт customdc.
16. В меню Action (Действие) выберите команду Set Description (Задать описание).
    Откроется окно Security Template Description (Описание шаблона безопасности).
17. В поле Description (Описание) наберите **Custom Security Template for Training** и щелкните кнопку OK.
18. В дереве консоли щелкните папку C:\WINNT\Security\Templates.
    Заметьте: в правой панели для customdc теперь отображается соответствующее описание.
19. Почитайте описания других шаблонов Windows 2000 Server.

▶ Задание 3: создайте новую базу данных системы безопасности

1. В дереве консоли щелкните пункт Security Configuration And Analysis (Анализ и настройка безопасности) и прочитайте текст в правой панели.
2. В меню Action (Действие) выберите команду Open Database (Открыть базу данных).
   Откроется диалоговое окно Open Database.
3. В поле File Name (Имя файла) наберите **training** и щелкните кнопку Open (Открыть).
   Откроется диалоговое окно Import Template (Импортировать шаблон).
4. Щелкните customdc.inf, а затем — кнопку Open (Открыть).
   Это тот шаблон, который Вы создали на предыдущем этапе.

▶ Задание 4: проанализируйте текущие параметры безопасности

Проанализируйте текущие параметры Server01 на соответствие созданному Вами шаблону.

1. Удостоверьтесь, что в дереве консоли выбран узел Security Configuration And Analysis (Анализ и настройка безопасности).
2. В меню Action (Действие) выберите команду Analyze Computer Now (Анализ компьютера).
   Откроется диалоговое окно Perform Analysis (Анализ), показывающее путь к журналу ошибок и его имя в следующем виде: C:\Documents and Settings\Administrator\Local Settings\Temp\training.log.
3. Щелкните кнопку OK.
   Открывшееся окно Analyzing System Security (Анализ безопасности системы) сообщит о проверке различных аспектов конфигурации безопасности ServerOl на соответствие Вашему шаблону.
4. Когда закончится анализ, раскройте узел Security Configuration And Analysis.
5. Раскройте узел Account Policies (Политики учетных записей) и щелкните узел Password Policy (Политика паролей).
   В правой панели для каждой политики отображены параметры шаблона и настройки компьютера. Несовпадения отмечаются красным кругом с крестом в центре. Совпадения отмечаются белым кругом с зеленой галочкой в центре. Если флажка или метки нет, то этот параметр безопасности не указан в шаблоне.
6. В дереве консоли щелкните узел Security Configuration And Analysis (Анализ и настройка безопасности).
7. В меню Action (Действие) выберите команду Configure Computer Now (Настроить компьютер).
   Откроется диалоговое окно Configure System (Настройка системы).
8. Щелкните кнопку OK.
9. В меню Action (Действие) выберите команду Analyze Computer Now (Анализ компьютера).
   Откроется диалоговое окно Perform Analysis (Анализ).
10. Щелкните кнопку OK.
П. Просмотрите параметры политики и удостоверьтесь, что столбцы Database Settings и Computer Setting совпадают.
12. Закройте оснастку Security.
    Откроется окно сообщения с предложением сохранить консоль.
13. Щелкните кнопку Yes (Да).
14. Если откроется окно сохранения шаблонов безопасности, щелкните кнопку Yes (Да).

Оснастка Group Policy

Параметры безопасности определяют поведение системы в отношении безопасности. Использование GPO в службах Active Directory позволяет администратору централизованно устанавливать необходимые уровни безопасности систем предприятия.

При определении настроек для GPO, содержащего несколько компьютеров, принимают во внимание организационный и функциональный характер сайта, домена или организационного подразделения (ОП). Например, уровни безопасности, нужные ОП отдела сбыта, могут сильно отличаться от ОП финансового отдела.

Оснастка Group Policy (Групповая политика) разрешает устанавливать параметры безопасности прямо в хранилище Active Directory. Папка Security Settings (Параметры безопасности) находится в узле Computer Configuration (Конфигурация компьютера) и узле User Configuration (Конфигурация пользователя). Параметры безопасности разрешают администраторам групповой политики устанавливать политики, которые ограничивают пользователям доступ к файлам и папкам, определяют количество неверных паролей, которое пользователь может вводить до того, как ему будет отказано во входе, управляют правами пользователя, в частности определяют, какие пользователи могут входить на сервер домена. О работе с оснасткой Group Policy и управлении групповыми политиками см. занятие 4 главы 7.

Резюме

Windows 2000 включает набор средств настройки параметров безопасности, позволяющих выполнять периодический анализ системы для контроля за сохранностью конфигурации, а также вносить изменения. Оснастка Security Configuration And Analysis (Анализ и настройка безопасности) позволяет задавать параметры безопасности локальной системы и проводить ее анализ. Она просматривает параметры безопасности вашей системы, анализирует их и дает рекомендации по модификации текущих системных параметров. Оснастка Security Templates (Шаблоны безопасности) позволяет создавать и устанавливать шаблоны безопасности для одного или более компьютеров. Оснастка Group Policy (Групповая политика) позволяет задавать параметры безопасности в хранилище Active Directory.

Занятие 5. Аудит в Microsoft Windows 2000

На этом занятии Вы изучите входящий в Windows 2000 аудит — инструмент для поддержания безопасности в сети. Аудит позволяет отслеживать действия пользователя и общесистемные события. Кроме того Вы узнаете о политиках аудита и о том, что необходимо учесть перед настройкой политики. Также Вы научитесь настраивать аудит для отдельных ресурсов и вести журналы безопасности.

Изучив материал этого занятия, Вы сможете:

- ✓ планировать стратегию аудита и определять, для каких событий осуществлять аудит;
- ✓ настраивать аудит для объектов Active Directory, файлов, папок и принтеров;
- ✓ использовать программу Event Viewer для просмотра журнала и анализа событий.

Продолжительность занятия — около 75 минут.

Обзор аудита в Windows 2000

Аудит в Windows 2000 — это процесс отслеживания действий пользователя и действий Windows 2000 (называемых событиями). Во время аудита Windows 2000 по Вашим указаниям записывает информацию о событиях в журнал безопасности. В этот журнал записываются попытки входа в систему с правильными и неправильными паролями, а также события, связанные с созданием, открытием, уничтожением файлов или других объектов. Каждая запись в журнале безопасности содержит сведения о:

- выполненном действии;
- пользователе, выполнившем это действие;
- событии, произошедшем при этом, а также о том, было ли оно успешно.

Использование политики аудита

Политика аудита определяет, какие типы событий Windows 2000 должна записывать в журнал безопасности на каждом компьютере. Этот журнал позволяет отслеживать указанные Вами события.

Windows 2000 записывает сведения о событии в журнал безопасности на том компьютере, на котором это событие имело место. Например, Вы можете настроить аудит так, что каждый раз, когда кто-то неудачно пытается войти в домен с какой-то доменной учетной записью, это событие записывалось в журнал безопасности на контроллере домена. Это событие записывается на контроллере домена, а не на компьютере, на котором была сделана попытка входа в систему, потому что именно контроллер домена пытался и не смог аутентифицировать вход в систему.

Вы можете настроить политику аудита на компьютере для:

- отслеживания успеха/неудачи событий, таких как попытка входа в систему, попытка определенного пользователя прочесть указанный файл, изменений учетной записи пользователя или членства в группе, а также изменений в Ваших параметрах безопасности;
- устранения или минимизации риска несанкционированного использования ресурсов,

Вы можете использовать оснастку Event Viewer (Просмотр событий) для просмотра событий, записанных Windows 2000 в журнал безопасности. Вы также можете архивировать журналы для выявления долговременных тенденций — например, для определения

интенсивности доступа к принтерам или файлам или для контроля попыток несанкционированного доступа к ресурсам.

Планирование политики аудита

Вы должны решить, на каких компьютерах вести аудит. По умолчанию аудит отключен, При определении компьютеров для аудита Вы должны также спланировать, что отслеживать на каждом компьютере. Windows 2000 записывает проверяемые события отдельно на каждом компьютере.

Вы можете вести аудит:

- доступа к файлам и папкам;
- входа в систему и выхода из нее определенных пользователей;
- выключения и перезагрузки компьютера с Windows 2000 Server;
- изменений учетных записей пользователей и групп;
- попыток изменения объектов Active Directory.

Определив, какие события проверять, Вы должны решить, отслеживать ли их успех и/или неудачу. Отслеживание успешных событий расскажет, как часто пользователи Windows 2000 или ее службы получают доступ к определенным файлам, принтерам и другим объектам. Это пригодиться при планировании использования ресурсов. Отслеживание неудачных событий может предупредить о возможных нарушениях безопасности. Например, многочисленные неудачные Попытки входа в систему с определенной учетной записью, особенно если они происходили вне обычного рабочего времени, могут означать, что некто, не имеюший прав доступа, пытается взломать систему.

При определении политики аудита руководствуйтесь такими принципами.

- Решите, нужно ли Вам отслеживать тенденции в использовании ресурсов системы. В этом случае запланируйте архивацию журналов событий. Это позволит увидеть изменения в использовании системных ресурсов и заблаговременно увеличить их.
- Почаще просматривайте журнал безопасности. Составьте расписание и регулярно просматривайте этот журнал, поскольку настройка аудита сама по себе не предупредит Вас о нарушениях безопасности.
- Сделайте политику аудита полезной и легкой в управлении. Всегда проверяйте уязвимые и конфиденциальные данные. Проверяйте только такие события, чтобы получить содержательную информацию об обстановке в сети. Это минимизирует использование ресурсов сервера и позволит легче находить нужную информацию. Аудит слишком многих событий приведет к замедлению работы Windows 2000.
- Проверяйте доступ к ресурсам не пользователей группы Users (Пользователи), а пользователей группы Everyone (Все). Это гарантирует, что Вы отследите любого, кто подсоединился к сети, а не только тех, для кого Вы создали учетную запись.

Внедрение политики аудита

Вы должны продумать требования аудита и настроить его политику. Настроив политику аудита на каком-либо компьютере, Вы можете вести аудит файлов, папок, принтеров и объектов Active Directory.

Настройка аудита

Вы можете выполнять политику аудита, основанную на роли данного компьютера в сети Windows 2000. Аудит настраивается по-разному для следующих типов компьютеров с Windows 2000:

- для рядового сервера домена, изолированного сервера или компьютеров с Windows 2000 Professional политика аудита настраивается отдельно для каждой машины; скажем, для аудита доступа пользователя к файлу на рядовом сервере следует установить на нем политику аудита;
- для контроллеров домена устанавливается одна политика аудита на весь домен; для аудита событий на контроллерах домена, таких как изменения объектов Active Directory, следует настроить групповую политику для домена, которая будет действовать на всех контроллерах.

Примечание Типы событий, которые Вы можете проверять на контроллере домена, те же, что и на обычном компьютере. Процедура аудита та же, но Вы должны использовать групповую политику для всего домена.

Требования для выполнения аудита

Настройка и администрирование аудита требует выполнения следующих условий:

- Вы должны иметь разрешение Manage Auditing And Security Log (Управление аудитом и журналом безопасности) для компьютера, на котором Вы хотите настроить политику аудита или просмотреть журнал аудита; по умолчанию Windows 2000 дает такие права группе Administrators (Администраторы);
- файлы и папки, подвергаемые аудиту, должны находиться на дисках NTFS.

Настройка аудита

Вы должны настроить:

- **политику аудита,** которая включает режим проверки, но не осуществляет аудит для конкретных объектов;
- аудит **для конкретных ресурсов,** т, е. указывать определенные отслеживаемые события для файлов, папок, принтеров и объектов Active Directory; Windows 2000 будет отслеживать и записывать в журнал эти события.

Настройка политики аудита

В первую очередь надо выбрать типы отслеживаемых событий. Для каждого события устанавливаются параметры настройки, показывающие, какие попытки отслеживать: успешные или неудачные. Вы можете настраивать политики аудита через оснастку Group Policy (Групповая политика).

Типы событий, которые могут проверяться в Windows 2000, представлены ниже.

Событие	Описание
События входа в систему с учетной записью	Контроллер домена получил запрос на проверку правильности учетной записи пользователя.
Управление учетной записью	Администратор создал, изменил или удалил учетную запись или группу. Учетная запись пользователя была изменена, включена или выключена, или пароль был установлен или изменен.
Доступ к службе каталогов	Пользователь получил доступ к объекту Active Directory. Вы должны указать конкретные объекты Active Directory для отслеживания этого типа события.
События входа в систему	Пользователь входил в систему и выходил из нее или подключился/не смог подключиться по сети к данному компьютеру.

(окончание)

Событие	Описание
Доступ к объекту	Пользователь получил доступ к файлу, папке или принтеру. Вы должны указать файлы, папки или принтеры для проверки. Режим проверки доступа к службе каталогов проверяет доступ пользователя к определенному объекту Active Directory. Режим доступа к объекту проверяет доступ пользователя к файлам, папкам или принтерам.
Изменение политики	Были сделаны изменения в пользовательских настройках безопасности, правах пользователя или политиках аудита.
Использование привилегий	Пользователь применил права, например, по изменению системного времени. (Сюда не включаются права, связанные с входом в систему и выходом из нее.)
Отслеживание процесса	Пользователь произвел действие. Эта информация полезна программистам, желающим отследить детали выполнения программы.
Системное событие	Пользователь перезагрузил или выключил компьютер, или произошло событие, влияющее на безопасность Windows 2000 или на журнал безопасности. (Например, журнал аудита переполнен, и Windows 2000 не смогла записать новую информацию.)

Для настройки политики аудита на рядовом сервере или обычном компьютере — не контроллере домена создайте свою консоль MMC и добавьте к ней оснастку Group Policy (Групповая политика). В дереве консоли выберите папку Audit Policy (Политика аудита) из узла Computer Configuration (Конфигурация компьютера) (рис. 11-18). Консоль покажет текущие параметры политики аудита на правой панели.

Изменения, сделанные в политике аудита компьютера, вступят в силу, когда произойдет одно из следующих событий:

- Вы инициализируете применение политики, набрав в командной строке **secedit / RefreshPolicy machine_policy** и нажав клавишу Enter;
- Вы перезагрузите компьютер; Windows 2000 применяет изменения, внесенные в политику аудита, после перезагрузки;
- произойдет обновление политики — применение параметров политики, включая политики аудита, к Вашему компьютеру; автоматическое обновление политики происходит через равномерные настраиваемые интервалы, по умолчанию — каждые 8 часов.

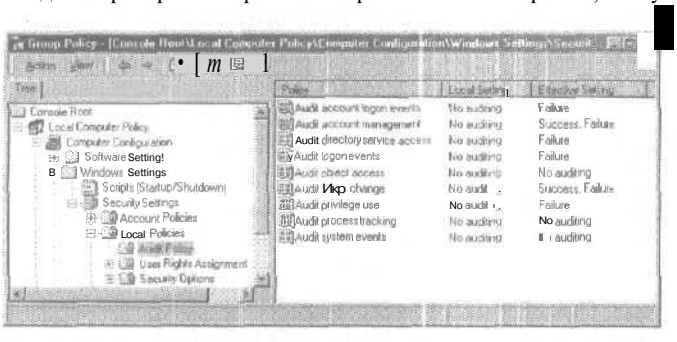


Рис. 11-18. Оснастка Group Policy (Групповая политика) с выбранной папкой Audit Policy (Политика аудита)

Аудит доступа к файлам и папкам

Аудит для файлов и папок можно устанавливать на разделах NTFS. Для аудита доступа пользователя к файлам и папкам, сначала надо включить режим политики Audit object access (Аудит доступа к объектам), включающий файлы и папки.

Установив режим проверки доступа к объектам в политике аудита, задайте аудит для определенных файлов и папок, указав, какие типы доступа и каких пользователей или групп подлежат проверке. Чтобы начать аудит файла или папки, откройте для этого объекта диалоговое окно свойств и на вкладке Security (Безопасность) щелкните кнопку Advanced (Дополнительно). Перейдите на вкладку Auditing (Аудит) и задайте параметры аудита для этого объекта.

Аудит доступа к объектам Active Directory

Для аудита доступа к объектам Active Directory надо включить политику аудита и настроить аудит для определенных объектов: пользователей, компьютеров, ОП или групп с указанием, какие типы доступа и доступ каких пользователей подлежат проверке.

Для установки аудита доступа к объектам Active Directory включите политику Audit directory services access (Аудит доступа к службе каталогов) в оснастке Group Policy (Групповая политика).

Для включения аудита определенных объектов Active Directory откройте оснастку Active Directory Users And Computers (Active Directory — пользователи и компьютеры) и выберите команду Advanced Features (Дополнительные функции) в меню View (Вид). Откройте диалоговое окно свойств для того объекта, который Вы хотите проверить. На вкладке Security (Безопасность) щелкните кнопку Advanced (Дополнительно). Перейдите на вкладку Auditing (Аудит) и задайте параметры аудита для этого объекта.

Аудит доступа к принтерам

Вы можете проверять доступ к принтерам, чтобы отслеживать доступ к уязвимым принтерам. Для установки аудита доступа к принтерам активизируйте политику Audit Object Access (Аудит доступа к объектам), которая включает и аудит принтеров. Затем установите аудит для конкретных принтеров и укажите, какие типы доступа и доступ каких пользователей подлежат аудиту. После выбора конкретного принтера сделайте то же, что и при установке аудита для файлов и папок.

Для установки аудита на принтер откройте диалоговое окно свойств для интересующего принтера. На вкладке Security (Безопасность) щелкните кнопку Advanced (Дополнительно). Перейдите на вкладку Auditing (Аудит) и установите параметры аудита для принтера.

Event Viewer

Программа Event Viewer (Просмотр событий) позволяет выполнять множество задач, включая просмотр журналов аудита, создающихся в результате установки политик аудита и проверяемых событий. Вы также можете использовать Event Viewer для просмотра журналов безопасности и поиска в них определенных событий.

Журналы в Windows 2000

Вы можете использовать Event Viewer (Просмотр событий) для просмотра журналов Windows 2000. По умолчанию в Event Viewer можно просмотреть три журнала:

Журнал	Описание
Журнал приложений	Содержит ошибки, предупреждения или информацию программ (базы данных или электронная почта). Записываемые события определяются разработчиком программ.
Журнал безопасности	Содержит информацию об успешных или неудачных проверяемых событиях. Записываемые события определяются политикой аудита.
Журнал системы	Содержит ошибки, предупреждения и дополнительную информацию, генерируемые Windows 2000. Перечень наблюдаемых событий задает Windows 2000.

Примечание Дополнительные службы могут добавить свои собственные журналы. Например, служба DNS записывает свои события в журнал DNS Server.

Обзор журнала безопасности

Журнал безопасности (Security log) содержит информацию о контролируемых политикой аудита событиях, таких как неудачные и удачные попытки входа в систему. Вы можете просматривать журнал безопасности в оснастке Event Viewer (рис. 11-19).

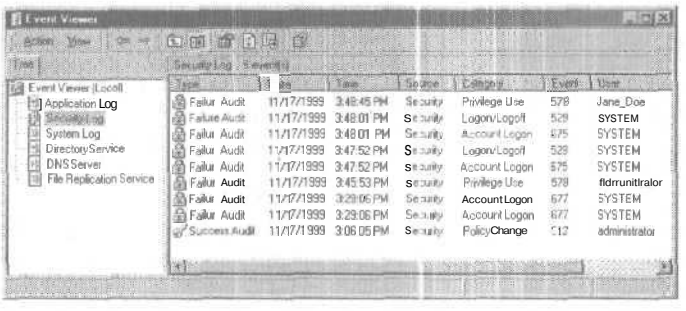


Рис. 11-19. Оснастка Event Viewer (Просмотр событий) с выбранным журналом Security Log (Журнал событий)

На правой панели Event Viewer отображается список журналов и сводная информация для каждого.

Успешные события символизирует «ключ», а неуспешные — «замок». Другая информация содержит дату и время произошедшего события, категорию события и пользователя, вызвавшего событие. Категория означает тип события: доступ к объекту, действие с учетной записью, доступ к службе каталогов или вход в систему.

Windows 2000 записывает события в журнал безопасности на том компьютере, где произошло событие. Вы можете просматривать эти события с любого компьютера, если у Вас есть соответствующие права. Для просмотра журнала безопасности на удаленном компьютере соответственно настройте Event Viewer при установке в консоль.

Поиск нужных событий

При первом запуске Event Viewer автоматически показывает все события, записанные в выбранный для просмотра журнал. Вы можете установить режим просмотра событий с помощью команды Filter (Фильтр). Также Вы можете находить определенные события с

помощью команды Find (Найти). Для этого после запуска Event Viewer в меню View (Вид) выберите команду Filter (Фильтр) или Find (Найти).

Управление журналами аудита

В Windows 2000 Вы можете отслеживать долговременные тенденции, архивируя журналы событий за разные периоды и сравнивая их. Это поможет узнать, как используются ресурсы и запланировать их расширение. Если есть проблема несанкционированного доступа к ресурсам, Вы можете использовать журналы для определения нарушителя. Windows 2000 позволяет задавать размер журналов и определять действие Windows 2000 при их переполнении.

Вы можете задавать свойства для каждого журнала аудита в отдельности. Для задания параметров журнала откройте в Event Viewer диалоговое окно его свойств.

Используйте это окно для каждого типа журнала для задания его длины, которая может составлять от 64 Кбайт до 4 194 240 Кбайт (4 Гб). По умолчанию длина равна 512 Кб. Свойства журнала позволяют также указать действие, предпринимаемое Windows 2000 при переполнении журнала.

Совет Параметры Event Viewer задаются в оснастке Security Configuration And Analysis (Анализ и настройка безопасности).

Архивация журналов

Сохранение журналов безопасности позволяет вести архив событий, связанных с безопасностью. Многие организации хранят архивные журналы в течение определенного времени для накопления информации о таких событиях. Если Вы хотите сохранить файл журнала, очистить его или открыть, выберите этот журнал в дереве консоли оснастки Event Viewer и выберите соответствующую команду в меню Action (Действие).

Резюме

Аудит в Microsoft Windows 2000 — это процесс отслеживания действий пользователя и Windows 2000 событиями, т. е. Windows 2000 по Вашему указанию добавляет запись о событии в журнал безопасности. Политика аудита определяет типы событий, записываемых в журнал на каждом компьютере. Журнал безопасности позволяет отслеживать указанные события. Вы должны определить, на каких компьютерах проводить аудит, и решить, что подвергать аудиту на каждом из них. Для проведения аудита нужно определить требования аудита и настроить его политику. Настроив политику аудита на компьютере, Вы можете проводить аудит для файлов, папок, принтеров и объектов Active Directory. Оснастка Event Viewer (Просмотр событий) используется для просмотра журналов аудита, создаваемых для проверяемых событий согласно параметрам политики аудита. Он используется также для просмотра файлов журнала безопасности и поиска определенных событий в журналах.

Закрепление материала

? J **Приведенные ниже вопросы помогут Вам** лучше **усвоить основные** темы данной **главы. Если Вы не** сумеете **ответить на вопрос,** повторите **материал** соответствующего **занятия. Правильные** ответы **см. в приложении «Вопросы и** ответы» в конце **книги.**

1. **Какой ключ предназначен для** создания цифровых **подписей — открытый или закрытый? Объясните ответ.**

2. **Какие способы удостоверения личности** могут **быть** использованы, если в **Вашей** сети компьютеры **клиентов с Windows** 2000 и Windows NT обращаются **за** аутентификацией **на серверы Windows** 2000 Server и Windows NT **Server?**

3. **Как с помощью шаблона безопасности упростить настройку и** анализ параметров **безопасности?**

4. **Как открыть Web-страницу для** работы **с сертификатами и для чего она** предназначена?

5. **Какие действия Вы должны предпринять для аудита определенных объектов на контроллерах домена, в котором** активна **групповая политика?**

ГЛАВА 12

Надежность и доступность

В этой главе

Коммерческая ОС должна обладать двумя основными качествами: надежностью и доступностью. В контексте ОС *надежность* (reliability) — способность сервера согласованно выполнять приложения и службы, а *доступность* (availability) — мера отказоустойчивости компьютера и его программ. Надежность растет по мере исключения потенциальных причин отказа системы, Доступность увеличивают, локализуя причины простоя. Иначе говоря, надежные и доступные системы отказоустойчивы, и их легко перезапустить после остановки. Мы рассмотрим обслуживание аппаратных устройств и драйверов, резервное копирование данных и защиту от сбоев. Кроме того, в этой главе приведен обзор способов аварийного восстановления.

Прежде всего

Для изучения материалов этой главы необходимо:

- установить Windows 2000 Server на Server01 и сконфигурировать его как контроллер домена;
- выполнить упражнения из предыдущих глав.

Занятие 1. Управление аппаратными устройствами и драйверами

К аппаратным средствам относится любое физическое устройство, связанное с компьютером и управляемое его микропроцессором. Для правильной работы устройства с Windows 2000 на компьютере надо установить соответствующий *драйвер устройства* (device driver) — программу, позволяющую устройству взаимодействовать с Windows 2000. Здесь кратко описаны аппаратные средства и рассказывается, как управлять устройствами и их драйверами, а также о средствах добавления, удаления и конфигурирования устройств и драйверов.

Изучив материал этого занятия, Вы сможете:

- ✓ управлять аппаратными устройствами и драйверами с помощью мастера Add/Remove Hardware (Установка оборудования) и оснастки Device Manager (Диспетчер устройств);
- ✓ применять пакеты исправлений (service pack).

Продолжительность занятия — около 40 минут.

Общие сведения об аппаратных средствах

Аппаратные средства включают в себя устройства, установленные на компьютере при его сборке, а также внешние устройства, добавленные позже: модемы, дисководы, дисковые контроллеры, приводы CD-ROM, принтеры, сетевые платы, клавиатуры, мониторы и видеоплаты.

Эти устройства могут поддерживать или нет спецификацию Plug and Play (PnP) и подключаться к компьютеру разными способами. Одни устройства, например сетевые адаптеры и звуковые платы, подключаются к разъемам расширения внутри компьютера, другие, скажем, принтеры и сканеры, — к портам на тыльной стороне системного блока. Ряд устройств, например платы PC, подключаются только к специальным разъемам на переносном компьютере.

Каждое устройство имеет уникальный драйвер, который обычно поставляется его изготовителем. Многие драйверы включены в комплект поставки Windows 2000.

Типы устройств

Windows 2000 классифицирует аппаратные устройства по типам. Типы аппаратных устройств включают видеоплаты, клавиатуры, приводы CD-ROM, порты и принтеры. Перечень типов устройств, установленных на компьютере, отображается в оснастке Device Manager и в мастере установки оборудования (рис. 12-1).

Каждый тип устройств включает список конкретных моделей. Например, тип модема включает более 200 модемов, которые Вы можете использовать в Windows 2000.

Устройства классифицируются и по способу подключения к ПК. Большинство устройств подключены постоянно и, как правило, устанавливаются только однажды. Они доступны всякий раз, когда Вы включаете компьютер:

- **звуковые** платы;
- видеоплаты;
- модемы;
- жесткие диски.

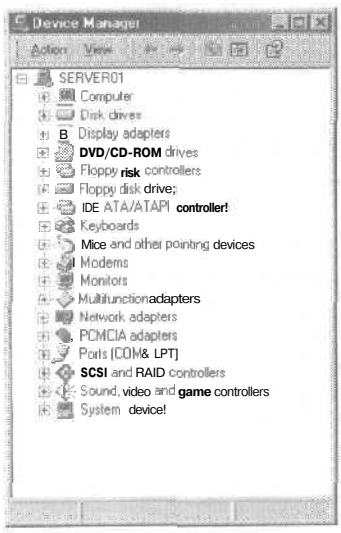


Рис. 12-1. Оснастка Device Manager (Диспетчер устройств)

Другие устройства подключаются и отсоединяются от компьютера по мере надобности. Вы можете подключать или вставлять такое устройство в соответствующий порт или разъем расширения, и Windows 2000 опознает и сконфигурирует его без перезагрузки компьютера. Отсоединяя такое устройство, Вы должны сообщить Windows 2000 только то, что Вы вынимаете его из разъема или отключаете. Выключать или перезагружать компьютер Вы не должны. Для «горячего» включения/отключения предназначены:

- платы PC, подключаемые к переносным компьютерам;
- аппаратные средства, подключаемые к шине USB или IEEE 1394;
- стыковочные станции, поддерживающие «горячую» стыковку и расстыковку переносных компьютеров;
- средства, подключаемые к последовательным или параллельным портам.

Полный список устройств, поддерживаемых Windows 2000, см. на Web-странице Microsoft HCL *http://www.microsoft.com*.

Общие сведения о Plug and Play

Спецификация *Plug and Play* (PnP) представляет собой набор технических требований, разработанных IEEE совместно с изготовителями компьютеров и программ Intel, Compaq, Microsoft и Phoenix Technologies. Совместимые с PnP устройства обнаруживаются и конфигурируются автоматически, для них также автоматически устанавливаются соответствующие драйверы. Установить PnP-устройство в Windows 2000 просто: его надо подключить к компьютеру и, если надо, обеспечить питание. Остальное сделает Windows: установит нужные драйверы, обновит параметры системы и выделит устройству ресурсы.

Например, можно подключить переносной компьютер к стыковочной станции и работать в сети, не изменяя конфигурации ОС. Позже Вы можете отключить компьютер от станции и работать в сети через модем, опять же без изменения конфигурации ОС. Windows 2000 автоматически настраивает драйвер устройства, чтобы он соответствовал новой аппаратной конфигурации.

PnP обеспечивает гладкое подключение любых новых устройств и надежную работу компьютера после их установки и удаления. PnP совместно с утилитой Power Options

(Электропитание) управляет питанием внутренних и периферийных устройств, отключая их или переводя в режим пониженного энергопотребления, когда они не используются. Если при установке/удалении устройства Вы работаете с какой-то программой, Windows сообщает об изменениях в конфигурации компьютера и предупредит о необходимости сохранить Вашу работу. Если при изменении конфигурации произойдет ошибка, она будет отражена в системном журнале.

Plug and Play и драйверы устройств

Windows 2000 автоматически устанавливает PnP-устройство и его драйвер. Впрочем, если Вы решите установить устаревший драйвер или устройство, возможности PnP будут задействованы лишь частично.

Применение PnP-драйверов для установки устаревших устройств может обеспечить ограниченную поддержку функций PnP. Хотя система не сможет сама распознать аппаратные средства и загрузить соответствующие драйверы, PnP способно наблюдать за установкой и распределять ресурсы, взаимодействуя с утилитой Power Options (Электропитание) из панели управления, и делать запись любых сбоев в системном журнале.

Вообще полностью автоматически установить устаревшее устройство практически невозможно — ряд параметров Вам придется настроить вручную. Для этого служат оснастка Device Manager или мастер Add/Remove Hardware.

Установка оборудования

Установка нового оборудования обычно включает три этапа:

1. подключение устройства к компьютеру;
2. установка соответствующих устройству драйверов;
3. конфигурирование параметров устройства.

Чтобы гарантировать правильную работу оборудования, следуйте инструкциям изготовителя. Для подключения устройства к соответствующему порту или слоту компьютера иногда требуется завершить работу и отключить компьютер.

Если устройство поддерживает PnP или оно необходимо для запуска системы, как, например, жесткий диск, то распознавание происходит автоматически. Ко для установки более сложных устройств, возможно, придется перезагрузить компьютер. После этого Windows 2000 попытается распознать новое устройство.

Если устройство не поддерживает PnP, Вам понадобится через оснастку Device Manager или мастер Add/Remove Hardware сообщить Windows 2000, какое устройство Вы устанавливаете. После распознавания устройства Вам будет предложено вставить установочный компакт-диск Windows 2000 или дискету изготовителя для загрузки нужных драйверов.

После установки драйверов устройства Windows 2000 сконфигурирует его параметры. Вы можете сделать это вручную, но желательно позволить Windows 2000 сделать это самой. Параметры, сконфигурированные вручную, будут фиксированными, т. е. изменить их в случае конфликта с другим устройством Windows 2000 не сможет.

Устройство подключается к порту или разъему компьютера согласно инструкции изготовителя. Возможно, понадобится перезагрузка. Для завершения установки нужно войти в систему как Administrator или член группы Administrators. Впрочем, если администратор уже загрузил драйверы для устройства, можно установить устройство и без привилегий администратора. Если компьютер подключен к сети, завершению процедуры может помешать сетевая политика.

Если для установки устройства надо перезагрузить компьютер, Windows 2000 после перезагрузки должна обнаружить устройство и запустить мастер установки оборудования. При установке устройства в слот компьютера завершите работу Windows и отключите пи-

тание компьютера. Открыв корпус системного блока, установите устройство в соответствующий слот. Закройте корпус и включите компьютер.

Если устройство установлено неправильно, оно, возможно, не поддерживает PnP. Чтобы установить драйверы для такого устройства, укажите путь к каталогу с его драйверами. Если устройство относится к типу SCSI, присоедините его к порту SCSI-контроллера согласно инструкциям изготовителя. Перезагрузите компьютер. Вы должны убедиться, что номер установленного SCSI-устройства не используется другим SCSI-устройством и что на устройстве правильно установлен терминатор. Чтобы изменить номер устройства в цепочке, обратитесь к инструкции изготовителя.

Примечание После установки плат PC и SCSI-устройств перезагружать компьютер обычно не надо. Описание установки см. в инструкции изготовителя. Сведения, изложенные в этой главе, используйте как общее руководство по установке устройств.

Чтобы установить устройство для шины USB или IEEE 1394, просто подключите его в любой порт USB или IEEE компьютера. Следуйте инструкциям, появляющимися на экране. При установке таких устройств Вам не нужно завершать работу системы или выключить компьютер. Хотя шины USB и IEEE 1394 похожи, они не взаимозаменяемы.

Удаление оборудования

Удаляемое PnP-устройство достаточно отключить. Для некоторых устройств надо сначала выключить компьютер. Чтобы убедиться в правильности своих действий, ознакомьтесь с инструкцией изготовителя по установке и удалению устройства.

Удалить несовместимое с PnP устройство поможет как мастер Add/Remove Hardware, так и оснастка Device Manager. После удаления устройства из системы Вы должны физически отсоединить или удалить его с компьютера. Например, если устройство подключено к порту на тыльной стороне системного блока, надо завершить работу системы, выключить компьютер, отсоединить устройство от порта и отключить шнур питания устройства (если таковой имеется).

Вместо удаления PnP-устройства, которое Вы потом будете подключать снова, например модема, его можно отключить временно. Физически устройство останется подключенным к компьютеру, но Windows 2000 модифицирует системный реестр так, чтобы при включении компьютера больше не загружать драйверы этого устройства. При включении устройства драйверы будут доступны снова. Отключение устройств удобно, если Вам надо иметь несколько аппаратных конфигураций. Несколько аппаратных конфигураций обычно применяются на мобильных компьютерах, которые подключаются и отключаются от стыковочной станции.

Примечание Оснастка Device Manager не удаляет драйверы устройства с жесткого диска — это делает мастер Add/Remove Hardware. Для определения лучшего способа удаления драйверов устройств изучите документацию его изготовителя.

Средства управления устройствами и драйверами

Для управления аппаратными устройствами и их драйверами предусмотрено несколько средств. К большинству из них можно обратиться через вкладку Hardware (Оборудование) диалогового окна System Properties (Свойства системы): в Control Panel откройте приложение System или, удерживая клавишу с флагом Windows, нажмите клавишу Break. В диалоговом окне System Properties перейдите на вкладку Hardware (рис.12-2).

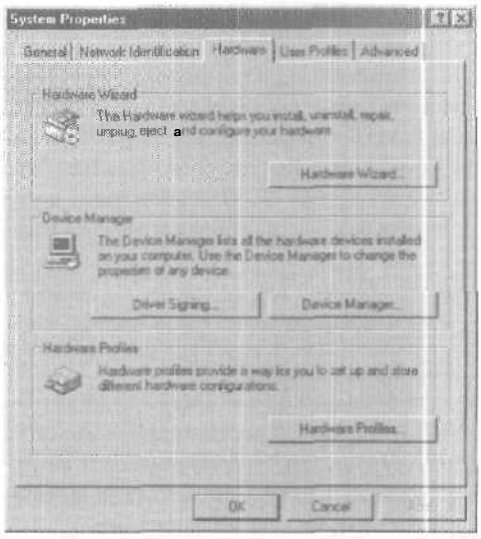


Рис. 12-2. Вкладка Hardware (Оборудование) диалогового окна System Properties (Свойства системы)

Отсюда Вы можете вызвать мастер Add/Remove Hardware, оснастку Device Manager, диалоговые окна Driver Signing Options (Параметры подписывания драйвера) и Hardware Profiles (Профили оборудования). Решить проблемы с аппаратными конфигурациями также поможет программа просмотра системных журналов Event Viewer.

Мастер Add/Remove Hardware

Позволяет добавлять новые аппаратные средства, отключать или удалять их из компьютера и решать проблемы с аппаратурой (рис. 12-3). Этот мастер можно вызвать, дважды щелкнув значок Add/Remove Hardware (Установка оборудования) в Control Panel.

Рис. 12-3. Мастер Add/Remove Hardware (Мастер установки оборудования)

Примечание Для вызова Add/Remove Hardware надо иметь права администратора. Утилита командной строки Runas позволяет работать в контексте защиты другой учетной записи пользователя. Если компьютер подключен к сети, сетевая политика может запретить вызов мастера.

Оснастка Device Manager

Device Manager (Диспетчер устройств) — это оснастка MMC, обеспечивающая графическое представление аппаратных средств, установленных на компьютере (рис. 12-1). Эту оснастку можно открыть из оснастки Computer Management (Управление компьютером), или создайте новую консоль MMC, содержащую оснастку Device Manager.

Оснастка Device Manager позволяет:

- определять, работают ли аппаратные средства на компьютере должным образом;
- изменять параметры аппаратуры;
- определять драйверы, загруженные для каждого устройства, и получать информацию по каждому драйверу;
- изменять дополнительные параметры и свойства устройств;
- устанавливать обновленные драйверы устройств;
- отключать, подключать и удалять устройства;
- определять конфликты устройств и вручную распределять используемые ими ресурсы;
- печатать отчет о системных ресурсах установленных устройств.

Обычно Device Manager применяется для контроля состояния оборудования и обновления драйверов устройств. Опытные пользователи могут с помощью Device Manager разрешать конфликты устройств и изменять параметры распределения ресурсов.

Внимание! Неправильное распределение системных ресурсов может стать причиной того, что подключенное устройство функционировать не будет, а компьютер будет сбоить или вообще не загрузится. Распределять ресурсы вручную должны только опытные пользователи.

Вам редко потребуется вручную перераспределять ресурсы, потому что эту задачу берет на себя Windows 2000. Кроме того, Device Manager позволяет управлять устройствами только на локальном компьютере, на удаленном же Device Manager работает в режиме «только для чтения».

Подписи драйверов

Позволяют Windows 2000 уведомлять пользователей, действительно ли драйвер, который они устанавливают, сертифицирован Microsoft (рис. 12-4) — к файлу драйвера, прошедшего испытания WHQL, присоединяется зашифрованная цифровая метка, подпись.

Цифровая подпись распознается Windows 2000 и связывается с конкретными пакетами драйверов. Этот процесс сертификации удостоверяет пользователей, что драйверы, которые они устанавливают, идентичны протестированным Microsoft, или уведомляет их об изменении файла драйвера после того, как он был протестирован HCL.

В окне Driver Signing Options предлагается 3 варианта проверки цифровой подписи драйвера:

- **Ignore (Пропустить)** — устанавливать все файлы независимо от подписи;
- **Warn (Предупреждать)** — уведомлять пользователя перед установкой неподписанного драйвера;
- **Block (Блокировать)** — запретить установку всех неподписанных драйверов.

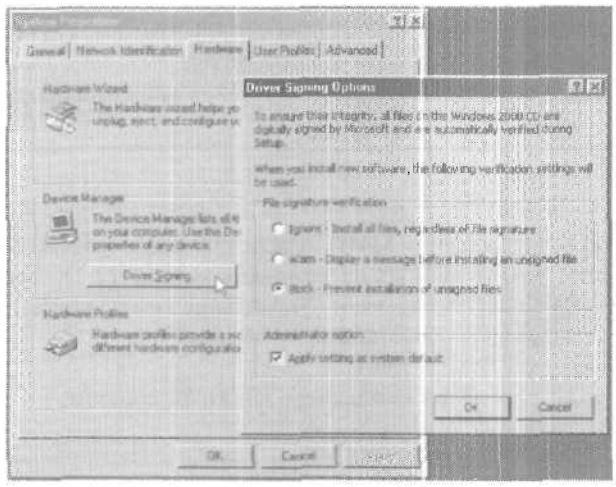


Рис. 12-4. Диалоговое окно настройки Driver Signing Options (Параметры подписывания драйвера)

По умолчанию в Windows 2000 вь бран вариант Warn.

Подпись не затрагивает программный код драйвера. Microsoft только помечает двоичный код драйвера, протестированного WHQL. Затем Microsoft создает файл каталога, содержащий код и криптографическую цифровую подпись. Результирующий двоичный файл создается так, что изменение его кода невозможно без изменения подписи файла каталога.

Примечание О цифровых подписях и криптографии см. главу 11.

Обычно хеш (шифр) двоичной и другой информации драйвера сохраняется в CAT-файле каталога, который и скрепляется цифровой подписью Microsoft. Сам двоичный код драйвера при этом не затрагивается, просто для каждого набора драйверов создается CAT-файл. Отношения между пакетом драйвера и его CAT-файлом описываются в INF-файле драйвера и поддерживаются системой после установки драйвера.

Поставщики, желающие получить подписанные драйверы, найдут сведения о подписи драйверов по адресу *http://www.microsoft.com/hwdev*,Web-страница обновления Windows, *http://windowsupdate.microsoft.com/default.htm*содержит только подписанные драйверы.

Примечание Чтобы применить параметры обработки подписи драйвера для всех пользователей, зарегистрируйтесь как администратор и пометьте в окне Driver Signing Options флажок Apply Setting As system default (Использовать в качестве системного параметра по умолчанию) (рис. 12-4). Параметры проверки подписи можно также определить в оснастке Group Policy, выбрав Unsigned Driver Installation Behavior (Поведение при установке неподписанного драйвера).

Профили оборудования

Это набор команд, сообщающий Windows 2000, какие устройства запустить при включении компьютера или какие параметры задать каждому устройству. При установке Windows 2000 создается конфигурация оборудования с именем Profile 1 (Current). По умолчанию название конфигурации для мобильных компьютеров — Undocked Profile (Current) (рис. 12-5).

По умолчанию все установленные на компьютере устройства включены в стандартный профиль оборудования. Профили оборудования особенно удобны, если у Вас переносной компьютер. Такие компьютеры обычно используют в разных местах, и профили позволяют менять набор устройств, подключенных к компьютеру в зависимости от его расположения. Например, у Вас может быть одна конфигурация по имени Docking Station Configuration для работы переносного компьютера в стыковочной станции с приводом CD-ROM и сетевой платой. И у Вас могла бы быть вторая конфигурация — Undocked для работы в гостинице или самолете, когда нужны не сетевая плата или привод CD-ROM, а модем и переносной принтер.

Профилями оборудования можно управлять: в Control Panel дважды щелкните значок System, перейдите на вкладку Hardware и щелкните кнопку Hardware Profiles. Если профилей несколько, можно определить стандартный профиль оборудования, который будет задействован при каждом запуске компьютера. Вы можете также настроить Windows 2000, чтобы выбирать нужный профиль на этапе загрузки. Включить/исключить устройство из профиля позволяет оснастка Device Manager. Если Вы исключили устройство из профиля, его драйверы не загружаются при запуске компьютера.

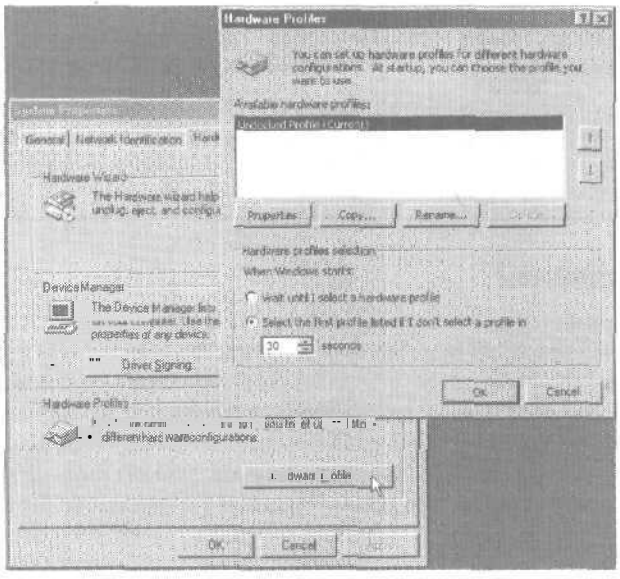


Рис. 12-5. Диалоговое **окно Hardware Profiles (Профили оборудования)**

Примечание Создавать, копировать, переименовывать или удалять профили оборудования на локальном компьютере имеет право лишь администратор.

Созданный после установки Windows 2000 профиль оборудования является прототипом для создания новых профилей. Для выбора профиля на этапе загрузки пометьте флажок Always Include This Profile As An Option When Windows Starts (Всегда выводить этот профиль как вариант при загрузке Windows) в диалоговом окне свойств профиля.

Журналы событий

Мониторинг системного журнала, заполняемого службой Event Log, помогает предсказывать и выявлять источники проблем в работе системы. Например, если в журнале есть

предупреждение, что дисковый накопитель читает или записывает в один из секторов на диске только после нескольких повторов, то данный сектор, по-видимому, будет вскоре окончательно испорчен.

Системный журнал и журнал приложений отражают проблемы, связанные с ПО. При сбое программы в журнале можно найти отчет о ее действиях до сбоя.

При диагностике с помощью журнала учтите эти рекомендации.

- **Архивируйте файлы событий в их собственном формате.** Двоичные данные, связанные с событием, будут сохранены, только если заархивировать файл событий в его собственном формате — .evt; в форматах .txt или .csv эти данные не сохраняются. Данные в двоичном коде помогают разработчику или специалисту технической поддержки определить источник проблемы.
- **Записывайте идентификаторы событий.** Эти номера соответствуют текстовому описанию в файле сообщений и помогают службе поддержки программного продукта понять причину сбоя.
- **Акцентируйте внимание на ошибках аппаратуры.** Если Вам кажется, что источником проблем является аппаратный компонент, выберите из журнала только те события, что относятся к нему.
- **Акцентируйте внимание на ошибках ОС.** Если характер сообщений указывает на проблемы с ОС, попытайтесь найти в журнале событий похожие сообщения и оцените частоту ошибок.

Примечание О журналах событий см. также файл \chapt12\articles\Monitoring Reliability.doc на прилагаемом компакт-диске.

Установка пакетов исправлений

В Windows NT/9x пакеты исправлений устанавливались отдельно после установки ОС. Windows 2000 поддерживает применение пакета исправлений в процессе установки ОС.

Windows 2000 также устраняет необходимость переустанавливать компоненты, установленные до применения пакетов исправлений. Это заметно облегчает жизнь при установке пакета исправлений в существующей системе, тогда как раньше при установке, например, пакета исправлений в Windows NT 4,0 приходилось преустанавливать службы типа IPX или RAS. В Windows 2000 эта проблема решена путем одновременной установки пакетов исправлений с ОС.

Установка пакета исправлений одновременно с ОС

Для установки нового пакета исправлений служит утилита update.exe с ключом /slip. Она копирует обновленные файлы из пакета исправлений поверх имеющихся. Заменяются файлы:

- layout.inf, dosnet.inf и txtsetup.sif, содержащие модифицированные контрольные суммы для всех файлов пакета исправлений; при установке новых системных файлов в эти файлы добавляются соответствующие записи;
- driver.cab, если были изменены драйверы в CAB-файле.

Установка пакета исправлений после установки ОС

Для этого надо запустить программу update.exe. При изменении конфигурации ОС (например, при удалении или добавлении служб) системе будет известно об установке пакета обновлений, какие файлы при этом были заменены или обновлены и откуда проводилась

установка. Так что нужные файлы с дистрибутива пакета исправлений и дистрибутива Windows 2000 на общем сетевом ресурсе, компакт-диске или Web-узле будут скопированы автоматически. Это устраняет необходимость переустанавливать пакет исправлений при любом изменении конфигурации системы.

После установки пакета исправлений при изменении конфигурации ОС (например, при добавлении службы RAS) всегда будут установлены правильные файлы — с дистрибутивов Windows 2000 или пакета исправлений. Это также устраняет необходимость повторно устанавливать пакет исправлений всякий раз после изменения конфигурации системы.

Резюме

К аппаратным средствам относится любое физическое устройство, подключенное к компьютеру и управляемое его микропроцессором. Драйвер позволяет устройству взаимодействовать с Windows 2000. Windows 2000 классифицирует устройства по типам. Совместимые с PnP устройства обнаруживаются и конфигурируются автоматически, для них автоматически устанавливаются драйверы. Установка устройства обычно идет в 3 этапа: подключение устройства к компьютеру, загрузка драйверов и конфигурирование параметров. PnP-устройство удаляется из системы обычно простым отключением от компьютера. Для удаления несовместимых с PnP устройств служат мастер Add/Remove Hardware и оснастка Device Manager. Для управления устройствами и их драйверами в Windows 2000 предусмотрен ряд средств. На вкладке Hardware диалогового окна System Properties можно вызвать мастер Add/Remove Hardware, оснастку Device Manager, диалоговые окна Driver Signing Options и Hardware Profiles. Решить проблемы с аппаратными конфигурациями помогает также программа Event Viewer. Пакеты исправлений можно разместить в сети, чтобы они автоматически применялись в ходе установки ОС.

Занятие 2. Резервное копирование

Цель резервного копирования — гарантировать эффективное и быстрое восстановление данных. Задание резервного копирования — это процедура архивирования данных. Регулярное копирование данных на жесткие диски сервера и жесткие диски клиентов сети предотвращает их потерю из-за отказов дисков, падений напряжения, заражения вирусом и т. п. Если такая потеря все же происходит, но Вы регулярно создавали резервные копии, Вы восстановите данные, файл или псе содержимое жесткого диска.

Изучив материал этого занятия, Вы сможете:

- ✓ выполнять резервное копирование данных на компьютере и в сети;
- ✓ планировать задание резервного копирования;
- ✓ настраивать утилиту резервного копирования Backup.

Продолжительность занятия — около 60 минут.

Утилита Backup

Утилита резервного копирования Backup (рис. 12-6), включенная в Windows 2000, позволяет архивировать и восстанавливать данные. Для ее запуска раскройте меню Start\Programs\Accesories\System Tools (Пуск\Программы\Стандартные\Служебные) и щелкните ярлык Backup (Архивация данных). Или в меню Start выберите команду Run, введите в открывшемся окне **ntbackup** и шелкните кнопку OK.

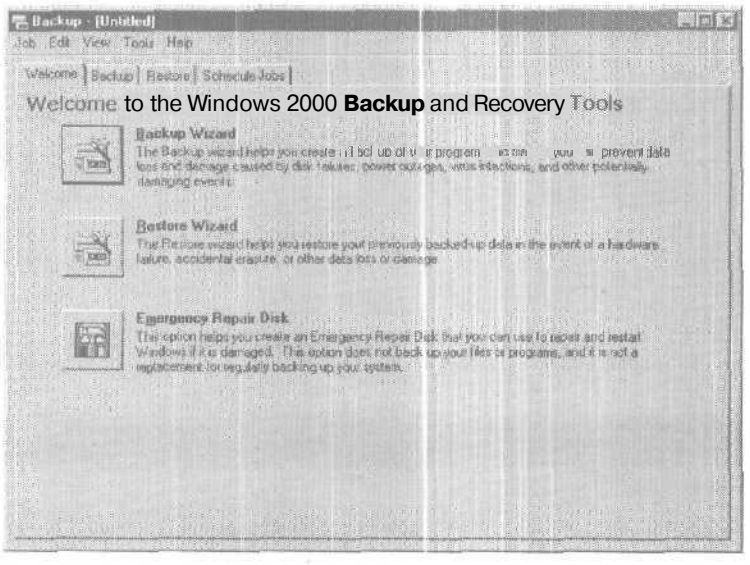


Рис. 12-6. Вкладка Welcome (Добро пожаловать) диалогового окна Backup (Архивация)

Backup позволяет копировать данные вручную или периодически создавать резервные копии в автоматическом режиме. Данные можно копировать в файл или на ленту. Файлы сохраняются на жестких дисках, съемных дисках (типа Iomega Zip и Jaz), записываемых компакт-дисках, оптических дисках и лентах.

Для успешного копирования и восстановления данных на компьютере с Windows 2000 Вы должны иметь соответствующие разрешения и права пользователя.

- Все пользователи могут копировать свои собственные файлы и папки. Они также могут копировать файлы, для которых они имеют разрешение Read (Чтение), Read and Execute (Чтение и выполнение), Modify (Изменить) или Full Control (Полный доступ).
- Все пользователи могут восстанавливать файлы и папки, для которых они имеют разрешение Write (Запись), Modify (Изменить) или Full Control (Полный доступ).
- Члены групп Administrators (Администраторы), Backup Operators (Операторыархива) и Server Operators (Операторы сервера) могут копировать и восстанавливать все файлы (независимо от установленных разрешений). По умолчанию члены этих групп имеют права на резервное копирование и восстановление файлов и каталогов.

Планирование резервного копирования

План резервного копирования должен включать способ восстановления данных. Что же принять во внимание при планировании?

Какие файлы и папки копировать

Всегда копируйте наиболее важные файлы и папки, например, отчет продаж и финансовые отчеты, системный реестр для каждого сервера и хранилище Active Directory.

Частота копирования

Копировать данные надо настолько часто, насколько часто они изменяются. Нет нужды делать ежедневные копии файлов, которые редко изменяются, например, ежемесячные или еженедельные отчеты.

На какой носитель сохранять архивы

Утилита Backup позволяет создавать архивы на следующих носителях.

- **Файлы.** Вы можете сохранять файлы на устройстве со сменными носителями типа Iomega Zip или в сети, например на файловом сервере. Созданный файл содержит заархивированные файлы и папки и имеет расширение .bkf. Пользователи могут копировать свои персональные данные на сетевой сервер.
- Магнитная лента. Этот более дешевый в сравнении с другими носитель прекрасно подходит для больших заданий резервного копирования из-за своей высокой емкости. Впрочем, ленты имеют ограниченный срок службы и могут со временем портиться. Для сохранения их эксплуатационных качеств следуйте рекомендациям изготовителя.

Примечание Если для резервного копирования и восстановления данных Вы используете устройство со съемным носителем, убедитесь, что оно включено в список Windows 2000 HCL.

Сетевое или локальное резервное копирование

Сетевая резервная копия может содержать данные от многих компьютеров сети. Это позволяет объединять дублирующие данные как от множества компьютеров, так и от единичных съемных резервных носителей информации. Такое копирование позволяет одному администратору сделать резервную копию всей сети. Выбор сетевого или локального резервного копирования зависит от данных, которые должны быть скопированы. Например, Вы можете копировать системный реестр и хранилище Active Directory только на том компьютере, где создаете архив.

Локальные резервные копии создаются на конкретном компьютере. Но прежде надо учесть некоторые особенности. Производить ли резервное копирование на каждом компьютере собственноручно или поручить архивирование пользователям? Обычно большинство пользователей архивирует свои данные нерегулярно. Надо оценить и количество доступных устройств со съемными носителями. Если у Вас накопители на магнитной ленте, надо иметь это устройство на каждом компьютере или последовательно перемешать его с компьютера на компьютер, чтобы создавать локальную резервную копию на каждом.

Вы можете комбинировать сетевое и локальное резервное копирование, скажем, когда нужные данные постоянно находятся на клиентских компьютерах и серверах, а устройства со съемными носителями есть не на всех. В этом случае пользователи сначала создают локальную резервную копию и затем копируют ее на сервер. Потом можно создать архивную копию данных на сервере.

Настройка параметров резервного копирования

Утилита Backup позволяет изменять стандартные параметры для всех заданий резервного копирования и восстановления. Эти параметры перечислены на вкладках диалогового окна Options (Параметры) (рис. 12-7). Чтобы открыть это окно, выберите команду Options в меню Tools (Сервис).

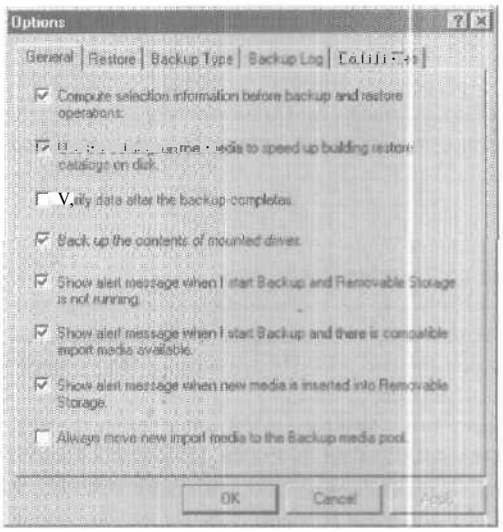


Рис. 12-7. Вкладка General (Общие) диалогового окна Options (Параметры)

Параметры архивирования вкладок окна Options таковы.

- Вкладка General (Общие). Включает параметры, касающиеся верификации данных, вывода сведений о состоянии заданий архивирования и восстановления, вывода сообщений об ошибках и содержания архива. Для проверки целостности скопированных данных пометьте флажок Verify Data After The Backup Completes (Проверять данные после завершения архивации).
- Вкладка Restore (Восстановление). Включает параметры, определяющие действия утилиты Backup, если имя восстанавливаемого файла идентично существующему.
- Вкладка Backup Type (Тип архива). Параметры, задающие стандартный тип архива. Выбор типа архива определяется тем, как часто Вы создаете резервные копии, насколько быстро хотите восстановить данные и какой объем Вы можете выделить для хранения архива.

- **Вкладка Backup Log (Журнал архивации).** Параметры, касающиеся детализации сведений, регистрируемых в журнале резервного копирования.
- **Вкладка Exclude Files (Исключение файлов).** Содержит список файлов, архивировать которые не надо.

Для конкретного задания резервного копирования стандартные параметры можно изменить, используя мастер Backup. Например, вместо стандартного типа архива Normal (Обычный) Вы вправе выбрать другой тип. Впрочем, при повторном запуске мастера Backup Вам будет вновь предложен заданный по умолчанию тип архива — Normal.

Типы резервного копирования

В Windows 2000 предусмотрено 5 способов резервного копирования: обычный, копирующий, разностный, добавочный и ежедневный. Стандартный тип архива задается на вкладке Backup Types диалогового окна Options (рис. 12-8).

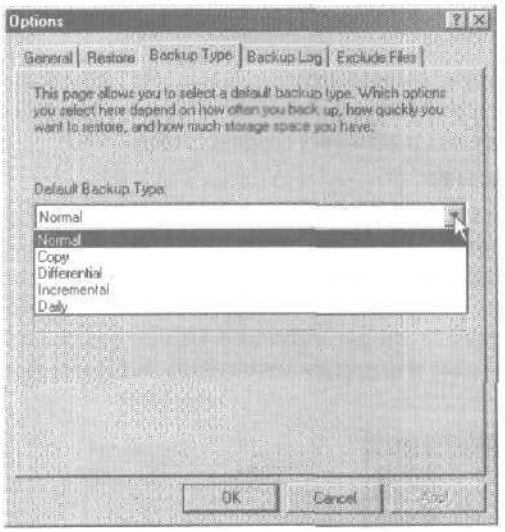


Рис. 12-8. Вкладка Backup Types диалогового окна Options

Некоторые способы резервного копирования используют маркеры, архивные атрибуты, которые устанавливаются у файлов, измененных с момента последнего архивирования. При резервном копировании эти атрибуты сбрасываются у всех архивируемых файлов до их следующего изменения.

Обычный ***архив***

При обычном, или полном, копировании архивируются все выбранные файлы и папки. Архивные атрибуты для выбора копируемых файлов не используются, но сбрасываются со всех заархивированных файлов. Обычное резервное копирование позволяет быстро восстановить данные, потому что копии файлов самые свежие и не надо восстанавливать данные из промежуточных архивов. Этот способ требует больше времени и больше места для хранения информации, чем любой другой.

Копирующий архив

Копируются все выбранные файлы и папки с сохранением архивных атрибутов. Используйте этот способ, если Вы не хотите сбрасывать архивные атрибуты, чтобы затем создать архив другого типа.

Разностный архив

Включает только файлы и папки с установленными архивными атрибутами. Так как в ходе разностного копирования архивные атрибуты не сбрасываются, при повторном копировании этого типа копируемый файл копируется дважды. Этот способ отличается скоростью архивирования и восстановления данных. Для полного восстановления информации из разностной копии надо сначала восстановить последний обычный архив, а затем – данные из разностного архива.

Добавочный архив

Включает только файлы и папки с установленными архивными атрибутами. После архивации эти атрибуты сбрасываются. При повторном копировании файл, если он не изменялся, вторично скопирован не будет. Этот способ позволяет очень быстро скопировать данные, но скорость восстановления будет невелика. Для полного «возрождения» информации надо восстановить последний обычный архив, а затем последовательно — все добавочные.

Ежедневный архив

Сюда включаются все выбранные файлы и папки, измененные в течение дня. Архивные атрибуты не сбрасываются. Используйте этот способ, если Вы хотите копировать все файлы и папки, которые изменяются в течение дня без изменения графика архивации.

Настройка способа архивации для конкретного задания

Для этого можно задействовать мастер Backup (рис, 12-9).

Вы можете задать тип резервного копирования для конкретного задания и без мастера. На вкладке Backup (Архивация) утилиты Backup, щелкните кнопку Start Backup (Архивировать). В окне Backup Job Information (Сведения о задании архивации), открывающемся после запуска резервного копирования, щелкните кнопку Advanced (Дополнительно). В окне Advanced Backup Options (Дополнительные параметры архивации) выберите тип архива из списка.

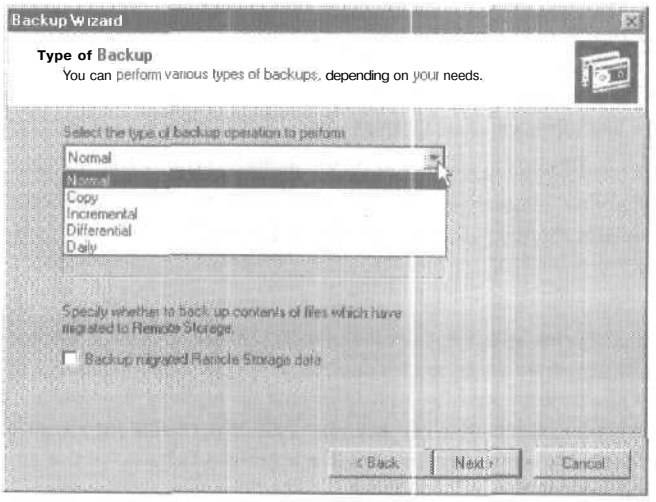


Рис. 12-9. Настройка способа архивации для конкретного задания

Комбинирование способов резервного копирования

Эффективная стратегия резервного копирования зачастую требует комбинирования разных способов архивации. Некоторые способы требуют больше времени для копирования,

но меньше — для восстановления данных, и наоборот. При комбинировании способов резервного копирования важно правильно проследить цепочку изменения архивных атрибутов файлов, поскольку они активно используются при создании добавочных и разностных архивов.

Ниже приведены примеры комбинирования способов резервного копирования.

- **Обычный + разностный. В** понедельник создается полный архив, а со вторника по пятницу — разностные. При создании последних архивные атрибуты не сбрасываются, т. е. каждая резервная копия будет включать все изменения, начиная с понедельника. Если данные потеряны в пятницу, Вы должны восстановить только обычную резервную копию, созданную в понедельник, и разностный архив за четверг. В результате требуется больше времени для копирования, но меньше — для восстановления.
- **Обычный** + добавочный. В понедельник создается полный архив, а со вторника по пятницу — добавочные. При создании последних архивные атрибуты сбрасываются, т. е. каждая резервная копия будет включать только те файлы, которые изменялись с момента предыдущего копирования. Если данные потеряны в пятницу, нужно восстановить полную копию от понедельника и все добавочные копии последовательно со вторника по пятницу. В результате копирование требует меньше времени, но восстановление — больше.
- **Обычный + разностный + копирующий.** Та же стратегия, что и в комбинации обычного и добавочного архивов, но в среду Вы создаете копирующий архив, который включает все выбранные файлы, не сбрасывает маркеры и не прерывает обычный график резервного копирования. Каждая разностная копия будет включать все изменения, начиная с понедельника. Копирующий архив, созданный в среду, не применяется для восстановления данных в пятницу. Копирующий архив полезен при создании текущей копии данных в обход расписания резервного копирования.

Архивирование данных

После составления плана резервного копирования, включая назначение его типа и времени, надо подготовить данные к копированию.

Предварительные операции

Во-первых, надо убедиться, что архивируемые файлы не используются. Утилита Backup не копирует файлы, заблокированные приложениями, поэтому сначала попросите пользователей закрыть файлы по электронной почте или из диалогового окна Send Console Message (Отправка сообщения консоли) в оснастке Computer Management.

Примечание Многие программы архивации других фирм создают резервные копии и открытых файлов.

Используя устройство со сменным носителем, убедитесь, что:

- устройство для резервного копирования подключено к сетевому компьютеру и его питание включено; если Вы копируете на магнитную ленту, подключите накопитель на магнитной ленте к компьютеру, на котором запускается Backup;
- устройство резервного копирования включено в Windows 2000 HCL;
- в устройство вставлен носитель информации; например, если Вы используете накопитель на магнитной ленте, убедитесь, что в него вставлена лента.

Выбор файлов и папок для копирования

Для запуска мастера резервного копирования запустите Backup и на вкладке Welcome (Добро пожаловать) щелкните кнопку Backup Wizard (Мастер архивации). Первым делом надо определить содержимое архива (рис 12-10).

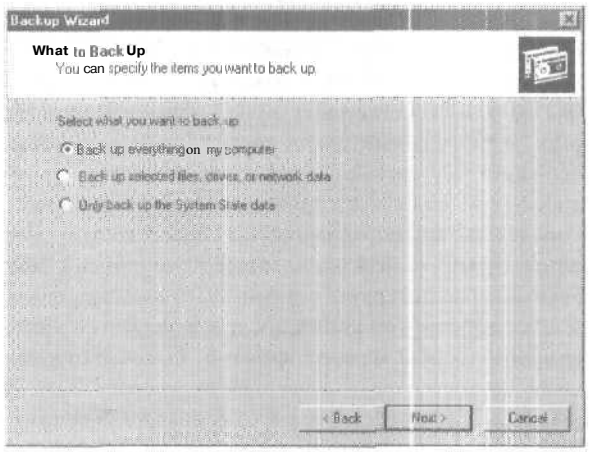


Рис. 12-10. Окно What To Back Up (Что следует архивировать) мастера архивации

Вы должны выбрать один из следующих вариантов.

- **Back Up Everything On My Computer (Архивировать все данные на этом компьютере).** Копируются все файлы компьютера, на котором запушена утилита Backup, кроме исключаемых по умолчанию, например некоторых файлов управления питанием.
- **Back Up Selected** Files, **Drives, Or Network Data (Архивировать выбранные файлы, диски или** сетевые данные). Копируются выбранные файлы и папки компьютера, на котором запушена Backup, и все общие файлы или папки в сети. Мастер отображает иерархию компьютеров в сети.
- **Only Back Up The System State Data (Архивировать только данные состояния системы).** Копируются системный реестр, хранилище Active Directory, папка SYSVOL, БД регистрации классов COM+, файлы запуска системы и службы сертификации (если установлены). Хранилище Active Directory и папка SYSVOL имеются только на контроллере домена. Используйте этот вариант для создания копии хранилища Active Directory, содержащего все объекты домена с их атрибутами. Остановите службы сертификации перед началом архивации, иначе Backup сообщит об ошибке. Копируются и восстанавливаются все данные о состоянии компьютера. Вы не можете копировать или восстанавливать отдельные компоненты данных состояния системы из-за их взаимосвязи.

Выбор устройства резервного копирования и параметры носителей информации

Выбрав данные для резервного копирования, надо задать устройство, где они будут сохранены.

Параметр	Описание
Backup Media Type (Тип носителя архива)	Целевой носитель, например лента или файл. Файл может располагаться на любом дисковом накопителе: жестком диске, общей сетевой папке или сменном диске типа Iomega Zip.

(окончание)

Параметр	Описание
Backup Media Or File Name (Носитель архива или имя файла)	Место, куда Backup будет сохранять данные. Для ленты вводят ее имя, а для файла — путь к файлу архива.

После задания параметров носителей информации мастер выводит список указанных параметров и предлагает варианты продолжения.

- **Начать архивацию.** Если щелкнуть кнопку Finish (Готово), начнется резервное копирование, и информация о его ходе будет отображаться в диалоговом окне Backup Progress (Ход архивации).
- **Указать дополнительные параметры архивации.** Если щелкнуть кнопку Advanced (Дополнительно), мастер позволит задать расширенные параметры, описанные в следующем разделе.

Примечание По окончании резервного копирования можно просмотреть отчет, который попадает в журнал архивации — текстовый файл на жестком диске компьютера, где регистрируются операции резервного копирования.

Дополнительные параметры архивации

Указывая дополнительные параметры, Вы изменяете значения параметров по умолчанию только для текущего задания. Следующие дополнительные параметры можно изменять.

Дополнительный параметр	Описание
Select The Type Ofjob. Backup Operation To Perform (Тип архива. Способы архивации)	Позволяет выбрать тип создаваемого архива: Normal (Обычный), Copy (Копирующий), Incremental (Добавочный), Differential (Разностный) и Daily (Ежедневный).
Backup Migrated Remote Storage Data (Архивирование данных из внешних хранилиш)	Резервное копирование данных, перемещенных диспетчером Hierarchical Storage Manager (HSM) во внешнее хранилище.
Verify Data After Backup (Проверять данные после архивации)	Подтверждает целостность скопированных данных. При этом проверяется идентичность данных, полученных при резервном копировании, с исходными. Рекомендуется задать этот параметр.
Use Hardware Compression, If Available (Использовать аппаратное сжатие)	Включает аппаратное сжатие данных для поддерживающих его накопителей на магнитной ленте.
If The Archive Media Already Contains Backups (Если носитель уже содержит архивы)	Определяет, заменять или добавлять текущую копию к существующей на устройстве резервного копирования. Для сохранения нескольких заданий резервного копирования выберите Append (Дозаписать этот архив к данным носителя). Если хранить предыдущие копии не надо, выберите Replace (Затереть данные носителя этим архивом).

(окончание)

Дополнительный параметр	Описание
Allow Only The Owner And The Administrator Access To The Backup Data And To Any Backups media (Разрешать доступ к данным этого архива и всем дозаписываемым на этот носитель архивам только владельцу и администратору)	Позволяет ограничить доступ к файлу или магнитной ленте с резервной копией. Параметр доступен, только если выбрана замена существующей копии на устройстве. При создании резервной копии реестра или хранилища Active Directory пометьте этот флажок для предотвращения несанкционированного копирования данных.
Backup Label (Метка архива)	Позволяет задать имя и описание для архива, они фиксируются в журнале архивации. Вы можете ввести понятное имя и описание, например: полная копия Sales, Сентябрь 14, 2000
Media Label (Метка носителя)	Позволяет задать имя для носителя информации, например, имя магнитной ленты. Вы можете указать имя для новых носителей информации, а также переписывать существующие, например можно задать метку «Копия хранилища Active Directory».
When To Back Up (Когда архивировать)	Now (Сейчас) или Later (Позже). При выборе biter можно указать имя задания, дату его начала и составить расписание.

В зависимости от времени копирования — Now (Сейчас) или Later (Позже) — мастер предлагает:

- закончить настройку и начать резервное копирование, в ходе которого отображаются сведения о выполнении задания;
- в дополнительных диалоговых окнах задать расписание резервного копирования, используя информацию из следующего раздела.

Расписание резервного копирования

Вы можете настроить автоматическое выполнение резервного копирования, которое будет сделано позже, например, когда все пользователи уже ушли с работы и файлы закрыты. Можно также задать регулярное копирование через равные промежутки времени. Windows 2000 поддерживает функциональность расписания, интегрируя Backup со службой Task Scheduler.

Для задания расписания архивации в окне When To Back Up (Когда копировать) мастера Backup щелкните переключатель Later (Позже). Откроется диалоговое окно Set Account Information (Указание учетной записи), где надо ввести Ваш пароль. Ваша учетная запись должна иметь соответствующие привилегии и разрешения для выполнения заданий резервного копирования.

Примечание Если служба Task Scheduler (Диспетчер задач) не запущена или для нее не указан параметр автостарта, Windows 2000 откроет диалоговое окно запуска службы. Щелкните кнопку OK, и откроется диалоговое окно Set Account Information.

Щелкните кнопку Set Schedule (Установить расписание), чтобы открыть диалоговое окно Schedule Job (Запланированное расписание). Вы можете установить дату, время и количество повторов архивации, например: каждую пятницу в 10 вечера. Вы также може-

те просмотреть все задания компьютера, щелкнув флажок Show Multiple Schedules (Показывать несколько расписаний). Это поможет предотвратить планирование разных задач на одно время. Щелкнув кнопку Advanced (Дополнительно), можно задать даты начала и окончания, а также регулярность выполнения задания.

После назначения расписания и завершения работы мастера задание помещается в календарь на вкладке Schedule Jobs (Запланированные задания) в утилите Backup. В назначенное Вами время задание начнет выполняться автоматически.

Совет Если на компьютере, предназначенном для резервного копирования, запущены службы сертификации (Certificate Services), Вы можете добавить в расписание их остановку перед началом резервного копирования, а по его окончании добавить их перезапуск. Простейший способ — создать и вставить командный файл в расписание Task Scheduler. Как это сделать, см. упражнение 1 этой главы.

Упражнение 1: резервное копирование файлов

С помощью мастера Backup Вы создадите резервные копии некоторых файлов на жестком диске. Затем, используя Task Scheduler, Вы создадите отложенное задание резервного копирования. Выполняйте это упражнение на Server01.

▶ Задание 1: создайте, **выполните и проверьте задание резервного копирования**

Для создания резервной копии файлов на локальном диске ServerOl Вы запустите утилиту Backup и поработаете с мастером архивации.

1. Зарегистрируйтесь на Server01 как Administrator с паролем **password.**
2. В меню Start (Пуск) выберите команду Run (Выполнить).
   Откроется диалоговое окно Run (Запуск программы).
3. В поле Open (Открыть) наберите **ntbackup** и щелкните кнопку OK.
   Откроется диалоговое окно Backup — [Untitled] (Архивация — [Безымянный]).
4. Прочтите описания трех вариантов работы с утилитой на вкладке Welcome (Добро пожаловать) и щелкните кнопку Backup Wizard.
   Откроется окно Welcome To The Windows 2000 Backup And Recovery Tools (Мастер архивации и восстановления Windows 2000).
5. Щелкните кнопку Next (Далее).
   Откроется окно What To Back Up (Что следует архивировать), где Вам предлагается выбрать копируемые данные.
6. Щелкните переключатель Back Up Selected Files, Drives, Or Network Data (Архивировать файлы, диски или сетевые данные), а затем — кнопку Next (Далее).
   Откроется окно Items To Back Up (Элементы для архивации), где надо выбрать локальные и сетевые диски, папки и файлы, которые будут включены в архив.
7. Раскройте узел My Computer (Мой компьютер).
8. Щелкните пункт System State (Состояние системы). Не щелкайте флажок слева от System State!
   На правой панели указано, что будут созданы резервные копии хранилища Active Directory, загрузочных файлов, реестра, базы данных регистрации классов COM+, папки SYSVOL и базы данных служб сертификации.
9. На левой панели окна раскройте узел диска C и щелкните букву C. Не щелкайте флажок слева от C:!

10. На правой панели пометьте флажок рядом с Boot.ini и щелкните кнопку Next (Далее). Откроется окно Where To Store The Backup (Где хранить архив).

Примечание Если к компьютеру не подключен накопитель на магнитной ленте, раскрывающийся список Backup Media Type (Тип носителя архива) будет недоступен. В этом случае File (Файл) — единственно доступный тип носителя для архива.

---

11. В поле Backup Media Or File Name (Носитель архива или имя файла) наберите **c:\backupl.bkf** и щелкните кнопку Next (Далее).

Примечание Обычно резервное копирование выполняется на ленту или в файл, сохраняемый на другой жесткий диск, устройство со сменным диском (типа Iomega Zip или Jaz), записываемый компакт- или оптический диск. Мы для простоты сохраним архив на то же устройство, где расположен файл, копия которого создается.

Откроется окно Completing The Backup Wizard (Завершение работы мастера архивации), где приведена сводка параметров задания.

12. Для задания дополнительных параметров щелкните кнопку Advanced (Дополнительно). Откроется окно Type Of Backup (Тип архива).
13. Просмотрите типы резервного копирования, перечисленные в списке Select The Type Of Backup Operation To Perform (Выберите нужный тип операции архивирования). Типы архивов были описаны выше.
14. Убедитесь, что выбран тип Normal (Обычный).
15. Убедитесь, что флажок Backup Migrated Remote Storage Data (Архивировать данные из внешних хранилищ) сброшен.

    Этот параметр включает поддержку возможностей HSM в Windows 2000 Server.
16. Щелкните кнопку Next (Далее).

    Откроется окно How To Backup (Способы архивации), где Вам предлагается включить проверку данных резервной копии после ее создания.
17. Пометьте флажок Verify Data After Backup (Проверять данные после архивации) и щелкните кнопку Next (Далее).

    Откроется окно Media Options (Параметры носителей), где Вам предлагается добавить текущую копию к существующей, либо перезаписать старую копию.
18. Пометьте флажок Replace The Data On The Media With This Backup (Затереть данные носителя этим архивом).

    Обратите внимание на флажок Allow Only The Owner And The Administrator Access To The Backup Data And Any Backups Appended To This Media (Разрешать доступ к данным этого архива и всем дозаписываемым на этот носитель архивам только владельцу и администратору). Этот параметр обеспечивает более высокий уровень безопасности. При его выборе восстановить данные из резервной копии сможет только владелец файла или Administrator (Администратор). Убедитесь, что этот флажок сброшен.
19. Щелкните кнопку Next (Далее).

    Откроется окно Backup Label (Метка архива), в котором вводится название задания резервного копирования и носителя архива.

    Мастер задает эти метки на основе текущей даты и времени.
20. В поле Backup Label (Метка архива) наберите Boot.ini **backup** set **created** on *<data>*, где *<data>* — текущая дата и время.

21. Не меняйте текст в поле Media Label (Метка носителя). Щелкните кнопку Next.
    Откроется окно When To Back Up (Когда архивировать), где предлагается начать резервное копирование немедленно или позже по указанному расписанию.
22. Убедитесь, что выбран переключатель Now (Сейчас). Щелкните кнопку Next.
    Откроется окно Completing The Backup Wizard (Завершение работы мастера архивации).
23. Для начала резервного копирования щелкните кнопку Finish (Готово).
    Откроется диалоговое окно Selection Information (Информация о выборе), где отображается краткая информация о размере копируемых данных и предполагаемой длительности копирования.
    Откроется диалоговое окно Backup Progress (Ход архивации), где отображается текущая информация о состоянии задания резервного копирования, примерном суммарном размере и текущем размере обработанных данных, текущем времени выполнения задания и времени, оставшемся до его завершения.
24. Увидев сообщение о завершении задания, щелкните кнопку Report (Отчет).
    Запустится программа Notepad со сформированным отчетом о произведенном резервном копировании. Отчет содержит основную информацию о задании резервного копирования: время его начала и количество скопированных файлов.
25. Закройте программу Notepad.
26. В диалоговом окне Backup Progress (Ход архивации) щелкните кнопку Close (Закрыть).
    Откроется диалоговое окно Backup — [Untitled] с открытой вкладкой Welcome.

► **Задание 2: создайте, выполните и проверьте автоматически выполняемые задание архивации**

Вы создадите отложенное задание резервного копирования с помощью Task Scheduler.

1. На вкладке Welcome (Добро пожаловать) щелкните кнопку Backup Wizard (Мастер архивации).
   После запуска мастера откроется окно Welcome To The Windows 2000 Backup And Recovery Tools (Мастер архивации и восстановления Windows 2000).
2. Щелкните кнопку Next (Далее).
   Откроется окно What To Back Up (Что следует архивировать), где надо выбрать данные, предназначенные для копирования.
3. Щелкните переключатель Back Up Selected Files, Drives, Or Network Data (Архивировать выбранные файлы, диски и сетевые данные) и щелкните кнопку Next.
   Откроется окно Items To Back Up (Элементы для архивации), где надо выбрать локальные и сетевые диски, папки и файлы, которые будут скопированы.
4. Раскройте узел My Computer (Мой компьютер), затем диск C и пометьте флажком папку Inetpub.
5. Щелкните кнопку Next (Далее).
   Откроется окно Where To Store The Backup (Где хранить архив), где надо выбрать расположение резервной копии.
6. В поле Backup Media Or File Name (Носитель архива или имя файла) наберите C:\backup2.bkf и щелкните кнопку Next (Далее).
   Откроется окно Completing The Backup Wizard (Завершение работы мастера архивации).
7. Для задания дополнительных параметров щелкните кнопку Advanced (Дополнительно).
   Откроется окно Type Of Backup (Тип архива), где Вам предлагается выбрать тип создаваемого архива.
8. Убедитесь, что в списке Type Of Backup Operation To Perform (Выберите нужный тип операции архивирования) выбрано Normal (Обычный).

9. Щелкните кнопку Next (Далее).

   Откроется окно How To Backup (Способы архивации).

10. Пометьте флажок Verify Data After Backup (Проверять данные после архивации) и щелкните кнопку Next (Далее).

    Откроется окно Media Options (Параметры носителей).

11. Щелкните переключатель Replace The Data On The Media With This Backup (Затереть данные носителя этим архивом).

12. Убедитесь, что флажок Allow Only The Owner And The Administrator Access To The Backup Data And Any Backups Appended To This Media (Разрешать доступ к данным этого архива и всем дозаписываемым на этот носитель архивам только владельцу и администратору) сброшен, и щелкните кнопку Next (Далее).

    Откроется окно Backup Label (Метка архива), предлагающее ввести метку архива и носителя.

13. В поле Backup Label (Метка архива) наберите **Inetpub backup set created on** *<data>*, где *<data>* — текущая дата и время.

14. Не изменяйте текст в поле Media Label (Метка носителя). Щелкните кнопку Next.

    Откроется окно When To Back Up (Когда архивировать).

15. Щелкните переключатель Later (Позже).

    Откроется диалоговое окно Set Account Information (Указание учетной записи), в котором надо ввести пароль учетной записи MICROSOFT\administrator. Если служба Task Scheduler не настроена для автозапуска, сначала откроется диалоговое окно с предложением запустить эту службу. Щелкните кнопку OK, после чего откроется диалоговое окно Set Account Information.

    Поскольку служба Task Scheduler автоматически запускает приложения, не проверяя параметров безопасности и прав пользователя компьютера или домена, нужно указать имя и пароль пользователя для запуска отложенного резервного копирования. Для назначенного задания архивации Вы должны быть членом группы Backup Operators (Операторы архива) с разрешениями доступа ко всем копируемым файлам и палкам.

    Для упрощения задачи при настройке задания архивации используйте учетную запись Administrator (Администратор).

16. Убедитесь, что в поле Run As (Пользователь) появился текст MICROSOFT\administrator. Затем в полях ввода пароля наберите password,

17. Щелкните кнопку OK,

18. В поле Job Name (Имя задания) наберите **Inetpub Backup** и щелкните кнопку Set Schedule (Установить расписание).

    Откроется диалоговое окно Schedule Job, в котором надо назначить время начала и параметры расписания резервного копирования.

19. В списке Schedule Task выберите Daily (Ежедневно), а в поле Start Time (Время начала) введите текущее время, прибавив к нему 5 минут.

20. Щелкните кнопку Advanced (Дополнительно).

    Откроется окно Advanced Schedule Options (Дополнительные параметры расписания).

21. Пометьте флажок End Date (Дата окончания), выберите в списке завтрашнюю дату и щелкните кнопку OK.

    Откроется окно Schedule Job (Запланированное задание).

22. Щелкните кнопку OK.

    Откроется окно When To Backup (Когда архивировать).

23. Щелкните кнопку Next (Далее).

Откроется окно мастера Completing The Backup Wizard (Завершение работы мастера архивации), отображающее сводку выбранных Вами параметров задания.

24. Для запуска задания резервного копирования щелкните кнопку Finish (Готово).

    Откроется диалоговое окно Backup — [Untitled] (Архивация — [Безымянный]) с открытой вкладкой Welcome (Добро пожаловать).

25. Закройте окно утилиты Backup.

    Задание резервного копирования запустится в назначенное время.

26. Запустите Windows Explorer (Проводник Windows), щелкните диск C: и убедитесь в наличии файла Backup2.bkf.

► Задание 3: просмотрите и настройте задания

Вы просмотрите назначенные задания резервного копирования и назначите новые.

1. Выберите Start\Accessories\System Tools (Пуск\Стандартные\Служебные) и щелкните ярлык Scheduled Tasks (Назначенные задания).

   Откроется одноименное окно. Заметьте, что в списке заданий присутствует Inetpub Backup.

2. Дважды щелкните значок задания Inetpub Backup.

   Обратите внимание на текст в поле Run (Выполнить). Это команда консольного приложения ntbackup с параметрами, сгенерированными мастером для архивации папки Inetpub.

   Если перед запуском резервного копирования надо остановить какую-либо службу, например Certificate Services, создайте командный файл (.cmd или .bat) с командами остановки службы, запуска задачи резервного копирования и последующего запуска остановленной службы. Команда для остановки службы Certificate Services:

   ```
   net stop «certificate services»
   ```

   а для запуска;

   ```
   net start «certificate services»
   ```

3. Щелкните вкладку Schedule (Расписание).

   В списке указано задание, созданное с помощью мастера Backup.

4. Чтобы закрыть окно Inetpub Backup шелкните кнопку OK.

   Откроется окно Scheduled Tasks (Назначенные задания).

5. В меню File (Файл) выберите команду Delete (Удалить).

   Откроется окно Confirm File Delete (Подтверждение удаления файла).

6. Щелкните кнопку Yes (Да).
7. Закройте окно Scheduled Tasks (Назначенные задания).

Резюме

Утилита Backup позволяет легко архивировать и восстанавливать данные. Вы можете использовать ее, чтобы копировать данные вручную или периодически создавать резервные копии в автоматическом режиме. Backup позволяет изменять стандартные параметры для всех операций резервного копирования и восстановления информации. В Windows 2000 предусмотрено 5 типов архивов: обычный, копирующий, разностный, добавочный и ежедневный. Перед началом резервного копирования надо убедиться, что копируемые файлы закрыты, и подготовить носители. Мастер архивации позволяет выбрать файлы и папки для копирования, назначить и настроить устройство резервного копирования, дополнительно настроить задание резервного копирования и указать для него расписание.

Занятие 3. Защита от сбоев

Сбоем называют любое событие, из-за которого компьютер не удается загрузить. Такими событиями могут быть разрушение главной загрузочной записи на жестком диске, удаление одного или нескольких файлов ОС, неисправность какого-либо устройства компьютера или всего компьютера. Сущность защиты от сбоев состоит в их предотвращении и сокращении времени простоя системы. Это достигается с помощью ИБЛ — *источников бесперебойного питания* (uninterruptible power supply, UPS) и отказоустойчивых дисковых конфигураций.

Изучив материал этого занятия, Вы сможете:

- ✓ настраивать ИБП для обеспечения резервного электропитания;
- ✓ создавать отказоустойчивые дисковые конфигурации.

Продолжительность занятия — около 40 минут.

Источник бесперебойного питания

Восстановление после сбоя (disaster recovery) — это восстановление работоспособности компьютера для обеспечения входа в систему и доступа к системным ресурсам. Очень часто сбой происходит из-за проблем с энергоснабжением. Серверы, как правило, защищены от этого типа сбоев. Компьютеры клиентов также можно защитить от отказов электросети.

ИБП обеспечивает резервное питание компьютера в случае отказа электросети. Время работы и потребляемая мощность резервного питания зависит от типа ИБП. В общем случае он должен обеспечить мощность на столько времени, чтобы его хватило для корректного завершения работы и выключения компьютера.

Примечание Для использования ИБП с Windows 2000 убедитесь, что устройство включено в Windows 2000 HCL.

Настройка параметров службы UPS

Для настройки службы UPS служит вкладка UPS (ИБП) диалогового окна Power Options Properties (Свойства: Электропитание). Чтобы открыть это окно, в Control Panel дважды щелкните значок Power Options (Электропитание). Для настройки службы надо указать:

- номер последовательного порта, к которому подключен ИБП;
- условия, при которых ИБП посылает сигналы: сбой электропитания, разряд аккумулятора, удаленное закрытие системы;
- время работы от аккумулятора, ею перезарядки и рассылки предупреждения об отказе электропитания.

Примечание Значения параметров службы UPS зависят от характеристик конкретного ИБП, подключенного к компьютеру. Подробности о назначении параметров см. в инструкции по эксплуатации ИБП.

Тестирование конфигурации ИБП

Настроив службу UPS на компьютере, протестируйте полученную конфигурацию, отключив основное питание. Во время теста компьютер и периферийные устройства, подклю-

ченные к ИБП, должны оставаться в рабочем состоянии. На экране и в системном журнале должно появиться сообщение о сбое питания.

Примечание Не рекомендуется тестировать ИБП на рабочем компьютере — лучше это сделать на резервной или специально выделенной машине. При использовании рабочего компьютера существует опасность потери информации, что может потребовать переустановки ОС. Помните: при внезапном отключении компьютера данные могут быть повреждены или потеряны.

Дождитесь разряда аккумуляторной батареи и убедитесь, что система была принудительно остановлена. Восстановите электропитание, откройте журнал событий и убедитесь, что в нем отражены все действия и нет ошибок.

Примечание Некоторые изготовители ИБП предоставляют собственное ПО, позволяющее использовать расширенные возможностям их устройств.

Отказоустойчивые диски

Отказоустойчивость (fault tolerance) — свойство компьютера или ОС противодействовать катастрофическим ситуациям вроде падения напряжения или неисправности оборудования без потерь данных и нарушения работоспособности. Полностью отказоустойчивые системы для предотвращения потерь данных применяют отказоустойчивые дисковые массивы.

Если данные размещены на отказоустойчивой системе, выполнять резервное копирование все же нужно — на случай потери данных из-за ошибочного удаления, пожара, кражи и т. п. Отказоустойчивый диск не заменит хорошо продуманную стратегию резервного копирования с использованием внешнего хранилища информации, гарантирующую восстановление большей части утраченной информации.

Если жесткий диск вышел из строя из-за отказа механической или электронной части. можно вернуть систему к жизни — заменить жесткий диск и восстановить информацию из архива. Впрочем, потеря доступа к данным на время замены жесткого диска и восстановления информации может вылиться в большие затраты времени и денег.

RAID-системы

Для сохранения доступа к данным при выходе из строя одного из жестких дисков Windows 2000 Server предоставляет программную реализацию отказоустойчивой технологии RAID. В RAID-системе информация записывается на несколько дисков. При выходе из строя одного из них потери информации не происходит. Существует программная и аппаратная реализация RAID.

Программный RAID

Windows 2000 поддерживает две программные реализации RAID: зеркальные тома (RAID 1) и чередующиеся тома с четностью (RAID 5), известные также как тома RAID-5. Однако создание новых томов RAID возможно только на динамических дисках.

Программный RAID защищает систему, пока не будет устранен первый отказ. Если произошел второй сбой, а данные после первого еще не восстановлены, Вы сможете восстановить информацию только из резервной копии.

Примечание При переходе с Windows NT 4.0 на Windows 2000 сохраняются созданные ранее зеркальные и чередующиеся тома. Windows 2000 обеспечивает их ограниченную поддержку, позволяя управлять этими томами и удалять их.

Аппаратный RAID

В аппаратных RAID-системах за создание и обновление информации избыточных томов отвечает интерфейс контроллера диска. Некоторые изготовители оборудования внедряют средства поддержки защиты информации с применением RAID в платы контролеров дисковых массивов. Производительность в сравнении с программной реализацией RAID в этом случае выше, так как эти решения ориентированы на конкретную аппаратуру и обходят аппаратные драйверы ОС, обеспечивающие отказоустойчивость. Кроме того, аппаратные реализации RAID обычно предоставляют такие возможности, как дополнительные отказоустойчивые RAID-конфигурации, «горячая» замена поврежденных жестких дисков и выделенная кэш-память для повышения производительности.

Примечание Полнота поддержки RAID на аппаратном уровне определяется изготовителем оборудования.

Выбирая аппаратную или программную реализацию RAID, помните:

- аппаратные реализации дороже программных;
- аппаратные реализации, как правило, обеспечивают более быстрый обмен данными с диском в сравнении с программными реализациями;
- аппаратные решения зачастую привязывают Вас к конкретному изготовителю;
- аппаратные системы допускают «горячую» замену поврежденных жестких дисков без отключения компьютера и его перезагрузки как в ручном, так и в автоматическом режиме.

Зеркальные тома

Поддержку зеркальных томов в Windows 2000 Server обеспечивает драйвер отказоустойчивости (Ftdisk.sys). При этом на каждый из двух физических дисков записывается одинаковая информация (рис. 12-11). Каждый том является членом зеркального тома. Создание зеркального тома повышает гарантию сохранности данных в случае отказа одного из членов зеркального тома.

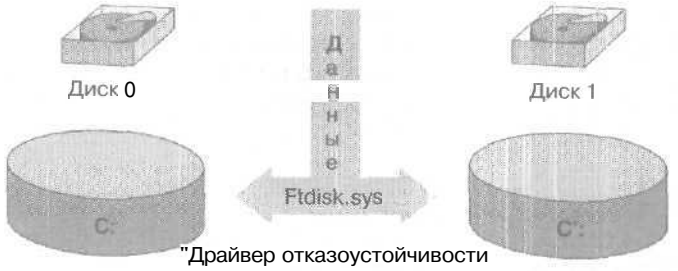


Рис. 12-11. Зеркальный том

Зеркальные тома могут содержать любые разделы, включая загрузочный или системный; однако оба диска в зеркальном томе должны быть динамическими.

Зеркальные тома могут быть распределены на нескольких дисках, Сушествуют стандартные конфигурации: RAID-10, RAID-1 и RAID-0. RAID-10 в отличие от RAID-0 явля-

ется отказоустойчивой конфигурацией RAID, потому что каждый диск в наборе также имеет зеркальную копию. RAID-10 увеличивает производительность дисковых операций.

Производительность зеркальных томов

Зеркальные тома повышают производительность операций чтения, поскольку драйвер отказоустойчивости производит чтение с обоих дисков тома одновременно. Производительность операций записи может несколько снижаться, потому что записывать приходится также на оба диска. После выхода из строя одного из дисков зеркального тома, производительность становится обычной, так как драйвер работает только с одним разделом.

Зеркальные тома дороги, потому что дисковое пространство используется на 50% (два диска для одного набора данных).

Внимание! С удалением зеркального тома теряется вся хранившаяся на нем информация.

Дублирование дисков

При повреждении контроллера, управлявшего работой обоих дисков в зеркальном томе, все его диски становятся недоступными. Вы можете установить на компьютере второй контроллер, чтобы у каждого диска в зеркальном томе был свой. Такая схема — дублирование дисков — защищает данные от выхода из строя одного из контроллеров или дисков. Некоторые аппаратные решения дублирования дисков используют два и более каналов одной платы контролера диска.

Дублирование уменьшает трафик шины и потенциально повышает производительность операций чтения. Дублирование дисков — это аппаратное расширение зеркального тома Windows 2000 и не требует дополнительной программной настройки.

Тома RAID-5

Windows 2000 Server поддерживает чередующиеся тома с четностью или контрольными суммами (RAID 5). Контрольная сумма — это математический метод определения количества четных и нечетных битов в числе или серии чисел, используемых для восстановления данных при утрате одного или нескольких чисел в последовательности.

В томе RAID-5 отказоустойчивость достигается за счет добавления информации о четности каждого дискового раздела, входящего в том (рис. 12-12). Если один из дисков выходит из строя, для восстановления его информации Windows 2000 использует данные и контрольные суммы на оставшихся дисках.

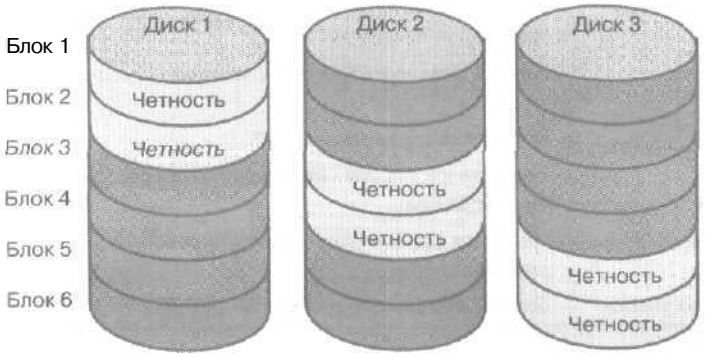


Рис. 12-12. Том RAID-5 с блоками контрольных сумм

Из-за вычисления контрольных сумм операции записи с применением RAID-5 медленнее, чем с зеркальными томами. Однако тома RAID-5 обеспечивают лучшую производительность, чем зеркальные тома, особенно при использовании нескольких контроллеров, так как данные распределяются по нескольким накопителям. При отказе диска скорость чтения падает на время, нужное Windows 2000 Server для восстановления данных с использованием контрольных сумм,

Тома RAID-5 дешевле в эксплуатации, чем зеркальные, так как более эффективно используется дисковое пространство. Чем больше дисков в томе RAID-5, тем меньше объем и стоимость хранения избыточной информации. Взгляните, как уменьшается объем для хранения избыточной информации после добавления в том RAID-5 дисков емкостью 2 Гб:

Количество дисков	Суммарный объем	Доступный объем	Избыточность
3	6 Гб	4 Гб	33%
4	8 Гб	6 Гб	25%
5	10 Гб	8 Гб	20%

У программно реализованных томов RAID-5 есть ограничения. Во-первых, тома RAID-5 могут содержать 3–32 диска. Во-вторых, программный том RAID-5 не может содержать системный или загрузочный разделы.

Windows 2000 не определяет аппаратные реализации RAID, поэтому ограничения, накладываемые на программную реализацию RAID не относятся к аппаратным конфигурациям.

Сравнение зеркальных томов с томами RAID-5

Зеркальные тома и тома RAID-5 обеспечивают разные уровни отказоустойчивости. Выбор той или иной конфигурации зависит от желаемого уровня защиты и стоимости оборудования. Главные отличия зеркальных томов (RAID-1) от томов RAID-5 — в их производительности и цене:

Зеркальные тома RAID-1	**Чередующиеся тома с четностью RAID-5**
Поддерживают FAT и NTFS	Поддерживают FAT и NTFS
Обеспечивают защиту системного и загрузочного разделов	Не обеспечивают защиту системного и загрузочного разделов
Требуют минимум два жестких диска	Требуют минимум 3 жестких диска (максимум 32 диска)
Высокая стоимость **хранения** мегабайта данных	Низкая стоимость хранения мегабайта данных
Избыточность 50%	**Избыточность** минимум 33%
Хорошая производительность при чтении данных	Удовлетворительная производительность при чтении данных
Хорошая производительность при записи данных	**Отличная производительность при записи данных**
Меньше использует системную память	Больше использует системную память

Скорость чтения и записи зеркальных томов сопоставима со скоростью работы отдельного диска. Тома RAID-5 достигают более высокой производительности при чтении, чем зеркальные тома, особенно в конфигурациях с несколькими контроллерами, за счет рас-

пределения данных по нескольким дискам. Однако необходимость вычисления контрольных сумм требует более высоких затрат компьютерной памяти, что замедляет скорость записи.

Зеркальные тома позволяют задействовать только 50% доступного объема диска, что повышает стоимость хранения I Мб данных в сравнении остальными системами. RAID-5 для хранения контрольных сумм задействует 33% доступного объема диска при использовании 3 дисков. При увеличении количества жестких дисков полезный объем дисков растет.

Внедрение RAID-систем

Программные средства отказоустойчивости в Windows 2000 Server реализованы только для динамических дисков. Вы можете создавать зеркальные и RAID-5 тома на программном уровне с помощью мастера Create Volume (Мастер создания тома), вызываемого из Computer Management. Откройте в этой оснастке папку Disk Management, и на правой панели появится подробная текстовая и графическая информация о физических дисках компьютера (рис. 12-13).

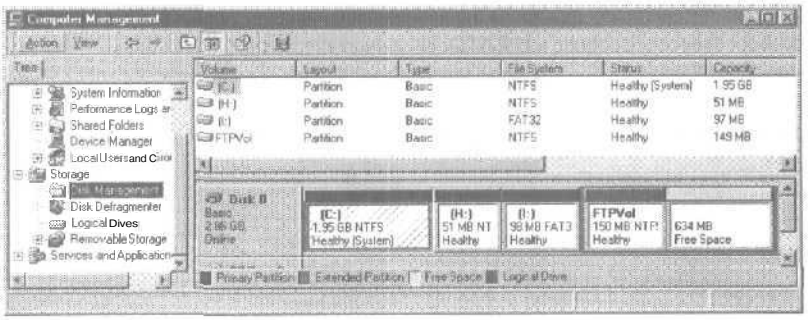


Рис. 12-13. Папка Disk Management (Управление дисками) в оснастке Computer Management (Управление компьютером)

Выберите нераспределенное пространство диска, в меню Action (Действие) выберите All Tasks (Все задачи), затем — команду Create Volume (Создать том) и следуйте указаниям мастера.

Примечание Windows 2000 Advanced Server и Windows 2000 Data Center для обеспечения более высокого уровня отказоустойчивости поддерживают кластеры. В данном курсе кластеры не рассматриваются.

Резюме

Защита от сбоев достигается за счет использования ИБП и отказоустойчивых дисков. ИБП обеспечивает питанием компьютер при перебоях в электросети. ИБП должен обеспечивать достаточную мощность на некоторый срок, чтобы предупредить о проблеме всех подключенных к серверу пользователей л принудительно завершить работу системы. Вы можете настроить службу UPS через вкладку UPS (ИБП) диалогового окна Power Options Properties (Свойства: Электропитание). Настроив службу UPS, протестируйте ее работу. Наряду с зашитой от перебоев питания дополнительный уровень зашиты информации обеспечивают отказоустойчивые RAID-системы. Для создания отказоустойчивых массивов дисков применяются аппаратные и программные средства. Поддержку зеркальных томов в Windows 2000 Server обеспечивает драйвер отказоустойчивости (Ftdisk.sys). При этом на каждый из двух физических дисков записывается одинаковая информация. Windows 2000 Server поддерживает чередующиеся тома с четностью (RAID-5). В RAID-5 отказоустойчивость достигается за счет подсчета контрольных сумм блоков данных на каждом дисковом разделе в томе. Скорость чтения и записи зеркальных томов сопоставима со скоростью работы отдельного диска. Производительность чтения томов RAID-5 выше, чем у зеркальных томов. Выгода от RAID увеличивается при использовании нескольких контроллеров (дублирующих дисков) из-за разделения ввода-вывода между несколькими каналами контроллеров, что повышает производительность и отказоустойчивость. Для создания зеркальных томов и томов RAID-5 служит мастер Create Volume из оснастки Computer Management.

Занятие 4, Восстановление после сбоев

Надежность и доступность подразумевает способность системы восстанавливаться после сбоев. На этом занятии Вы узнаете о восстановлении ОС Windows 2000, информации, зеркального тома или тома RAID-5.

Примечание О надежности и доступности Windows 2000 см. также статью \chapt12\articles\Win2000Reliability.doc на прилагаемом компакт-диске.

Изучив материал этого занятия, Вы сможете:

- ✓ использовать безопасный режим, консоль восстановления и диск ERD;
- ✓ восстанавливать сохраненные данные;
- ✓ восстанавливать тома RAID-5 или RAID-1.

Продолжительность занятия — около 60 минут.

Восстановление Windows 2000

В Windows 2000 несколько средств восстановления отказавшей ОС. Они полезны в случаях ошибочного удаления системных файлов или при решении проблем с ПО или драйвером устройства, послужившим причиной отказа. Windows 2000 предусматривает 3 способа восстановления работоспособности системы: безопасный режим, Recovery Console (Консоль восстановления) и диск аварийного восстановления системы (Emergency Repair Disk, ERD).

Примечание Вы можете переустановить Windows 2000 поверх поврежденной системы или установить Windows 2000 в другую папку. Это может занять некоторое время, но помогает в тех случаях, когда процесс аварийного восстановления не решил проблемы. При переустановке можно потерять изменения, сделанные в системе, например результаты применения пакетов обновления.

Безопасный режим

Безопасный режим (Safe mode) запускает систему с минимальным набором драйверов устройств и служб. Например, если новые драйверы устройств или ПО мешают загрузке системы, Вы можете перейти в безопасный режим и удалить их из системы. Безопасный режим не работает при повреждении или потере системных файлов или повреждении жесткого диска.

В безопасном режиме Windows 2000 использует параметры по умолчанию: VGA-монитор, драйвер мыши Microsoft и минимальный набор драйверов устройств, необходимый для запуска Windows. Если при загрузке в безопасном режиме проблемы исчезли, измените значения параметров по умолчанию и удалите лишние драйверы до полного решения проблемы,

При запуске в безопасном режиме Вы можете выбрать один из следующих параметров.

- Safe **Mode (Безопасный режим).** Запуск Windows 2000 с применением только основных файлов и драйверов (мыши, монитора, клавиатуры, накопителей, базового видеодрайвера, без поддержки сети). Если компьютер не загрузился в безопасном режиме, восстановите систему с помощью диска ERD.

- **Safe Mode With Networking (Безопасный режим с загрузкой сетевых драйверов).** Запуск Windows 2000 с основными файлами и драйверами и поддержкой сети.
- **Safe Mode With Command Prompt (Безопасный режим с поддержкой командной строки).** Запуск Windows 2000 с основными файлами и драйверами. После входа в систему вместо рабочего стола меню Start и панели задач появляется приглашение командной строки.
- **Enable Boot Logging (Включить протоколирование загрузки).** Запуск Windows 2000 с записью в файл названий всех загруженных (или незагруженных) установленных драйверов и служб. Файл называется ntbtlog.txt и находиться в папке %systemroot%. В режимах Safe mode, Safe mode with Networking и Safe mode with Command Prompt в список загрузки добавляются названия всех загружаемых драйверов и служб. Список загрузки удобен для выявления проблем загрузки системы.
- **Enable VGA Mode (Включить режим VGA).** Запуск Windows 2000 с использованием базового VGA-драйвера. Этот режим применяют, если новый драйвер видеоплаты мешает нормальной загрузке Windows 2000. Базовый видеодрайвер всегда используется при запуске системы в безопасном режиме (Safe mode, Safe mode with Networking или Safe mode with Command Prompt).
- **Last Known Good Configuration (Загрузка последней удачной конфигурации).** Запуск Windows 2000 с использованием содержимого системного реестра, сохраненного при последнем выходе из системы. **Выбирайте** этот режим в случаях неправильной настройки. Он не решает проблем, вызванных разрушением, несовместимостью или отсутствием драйверов или файлов. Будут потеряны и любые изменения, сделанные со времени последней успешной загрузки системы.
- **Directory Service Restore Mode (Восстановление службы каталогов).** Используется для восстановления папки SYSVOL и Active Directory на контроллере домена. Режим доступен только на контроллерах домена.
- **Debugging Mode (Режим отладки).** Запуск Windows 2000 с передачей отладочной информации через последовательные порты на другой компьютер. Режим важен для разработчиков ПО.

Если для установки Windows 2000 использовались Remote Install Services (Службы удаленной установки), в списке будут дополнительные режимы, позволяющие восстановить систему с помощью этих служб.

Для запуска Windows 2000 в безопасном режиме перезагрузите компьютер, удерживая клавишу F8. Перемещая подсвеченный курсор клавишами-стрелками, выберите нужный режим и нажмите клавишу Enter.

Безопасный режим поможет диагностировать возникающие проблемы. Если после старта в безопасном режиме симптомы проблемы исчезли, установите стандартные параметры и минимум драйверов устройств. Если вновь установленное устройство или драйвер вызвали проблемы, в безопасном режиме можно удалить драйвер из системы или отменить сделанные изменения.

Recovery Console

Текстовый интерпретатор команд Recovery Console отличается от командной строки Windows 2000. Он позволяет администратору получить доступ к жесткому диску Windows 2000-компьютера независимо от файловой системы (NTFS или FAT). Использовать Recovery Console при старте Windows 2000 не обязательно — консоль пригодится в случае невозможности загрузить компьютер.

Recovery Console позволяет получить ограниченный доступ к томам NTFS. FAT16 и FAT32 без запуска графического интерфейса, а также запускать/останавливать службы и восстанавливать систему специалистам из службы поддержки Microsoft. Recovery Console

поможет восстановить главную загрузочную запись и загрузочный сектор диска, а также отформатировать тома. Для запуска Recovery Console надо ввести пароль администратора.

Запуск Recovery Console

Для запуска Recovery Console загрузите компьютер с установочного компакт-диска Windows 2000 или с загрузочных дискет Windows 2000. Если у Вас нет загрузочных дискет и компьютер не может загружаться с компакт-диска, создайте набор загрузочных дискет на другом компьютере посредством утилит Makeboot.exe или Makebt32.exe.

Доступ к Recovery Console на локальном жестком диске можно получить и из меню загрузки Windows 2000. При разрушении главной загрузочной записи или загрузочного сектора для доступа к Recovery Console надо загрузиться с загрузочных дискет или компакт-диска. Чтобы добавить Recovery Console в меню Start, выберите команду Run (Выполнить), в открывшемся окне наберите *<cdrom>*:\I386\Winnt32.exe/cmdcons, где *<cdrom>* — буква привода CD-ROM.

Установка Recovery Console требует около 7 Мб дискового пространства на системном разделе.

Внимание! Установить Recovery Console на компьютер с зеркальным томом нельзя — сначала надо отменить зеркальное отражение. После установки зеркальный том можно создать снова.

Если Recovery Console не установлена, запустите Windows 2000 Setup. Нажмите клавишу Enter, для восстановления Windows 2000 нажмите клавишу R, а затем — клавишу C для входа в Recovery Console.

Некоторые параметры могут влиять на порядок использования Recovery Console:

- если на компьютере несколько ОС Windows 2000/ NT 4.0 и более ранних версий, они отобразятся в меню запуска Recovery Console;
- зеркальные тома отображаются в меню запуска Recovery Console дважды, но имеют одни и те же буквенные имена устройств и используются как одно устройство;
- изменения, сделанные Recovery Console на одном зеркальном томе, отражаются и на другом.

Для доступа к диску из Recovery Console введите порядковый номер восстанавливаемой ОС Windows 2000. Recovery Console предложит ввести пароль администратора. Если нажать Enter, не введя номер системы, Recovery Console закончит свою работу и перезагрузит компьютер.

Примечание Recovery Console не позволит получить доступ к компьютеру без пароля администратора выбранной ОС. После троекратного ввода неправильного пароля происходит выход из Recovery Console и перезагрузка компьютера. Для разрешения автоматического входа с правами администратора Вы можете использовать оснастку Group Policy (Групповая политика) или Security Configuration And Analysis (Анализ и настройка безопасности). Для этого надо в узле Security Options (Параметры безопасности) включить параметр Recovery Console: Allow automatic administrative logon (Консоль восстановления: разрешить автоматический вход администратора).

После ввода и проверки пароля Вам будет предоставлен полный доступ к Recovery Console и ограниченный доступ к жесткому диску. Вам будут доступны такие разделы и папки компьютера:

- %systemroot% и подпапки текущей версии Windows 2000;
- корневые папки всех разделов, включая %systemdrive%, привод CD-ROM и дискет с некоторыми ограничениями; об ограничениях при работе с дискетами см. ниже.

Примечание Если разрешено использование команды Set, Вы сможете копировать файлы на сменные носители информации, отключать подтверждения при копировании файлов, применять метасимволы в команде Copy для имен файлов и получить доступ ко всем системным папкам. Set -- необязательная команда Recovery Console. Ее можно активизировать из оснастки Group Policy (Групповая политика) или Security Configuration And Analysis (Анализ и настройка безопасности).

Recovery Console запрещает доступ к другим папкам (вроде Program Files или Documents And Settings) и папкам, содержащим другую установку Windows 2000. Доступ к другой установке обеспечивает команда logon. Еще способ — перезапустить Recovery Console и выбрать нужную ОС из меню с вводом соответствующего этой системе пароля администратора.

Вы не сможете скопировать какой-либо файл с жесткого диска компьютера на дискету. Копировать файлы разрешено только с дискеты или компакт-диска на жесткий диск либо с одного жесткого диска на другой. Скопировать файлы на съемный носитель можно, если разрешено использование команды Set. При попытке выполнить неправильную команду Recovery Console сообщит о запрете доступа.

Внимание! Команда Set позволяет вести запись на дискеты, а также открывает доступ к переменным окружения и дополнительным функциям Recovery Console. Чтобы разрешить пользователю изменять установленные по умолчанию переменные окружения Recovery Console, надо соответствующим образом настроить политику.

Recovery Console запоминает предыдущие введенные команды и позволяет выбирать их пользователю клавишами-стрелками «вверх» и «вниз». Для редактирования предыдущей команды используйте клавишу Backspace. Удалите ненужную часть команды и введите ее измененную часть. В любой момент Вы можете выйти из Recovery Console и перезапустить компьютер, введя в командной строке **exit**. Помните; Recovery Console может расставить буквенные имена дисков иначе, чем они размечены при работе в Windows 2000. Если при копировании файлов возникли проблемы с определением букв дисков, проверить правильность задания исходного и целевого дисков поможет команда Map.

Совет Список команд Recovery Console выводит команда Help. Ключ /?, указанный после имени команды, позволяет просмотреть ее назначение, синтаксис, различия в ее параметрах и др.

Диск аварийного восстановления

Если Вам не удалось загрузить систему в безопасном режиме и нет доступа к Recovery Console, можно обратиться к ERD, мастер создания которого есть в утилите Backup. При крахе системы сначала попытайтесь загрузиться с компакт-диска или загрузочных дискет Windows 2000, созданных утилитами Makeboot.exe или Makebt32.exe. Их можно запустить из папки Bootdisk установочного компакт-диска Windows 2000. При загрузке с дискеты два раза нажмите клавишу R, чтобы перейти в окно параметров восстановления. Используйте ERD для восстановления основных системных файлов. Заметьте: ERD не решит всех проблем, связанных с восстановлением диска.

Создавайте ERD при правильном функционировании компьютера, чтобы при необходимости подготовиться к восстановлению системных файлов. ERD позволяет решить проблемы с загрузкой компьютера, т. е. проблемы с реестром, системными файлами, сектором загрузочного раздела и начальном системном окружении. ERD не выполняет резерв-

ного копирования данных или программ и не заменяет регулярного резервного копирования системы.

В отличие от диска **ERD** для Windows NT в ERD для Windows 2000 нет копий файлов реестра. Как и в Windows NT, они находятся в папке %systemroot%\Repair. Однако эти файлы взяты с оригинальной установки Windows 2000. Их можно использовать для восстановления работоспособности компьютера.

При архивации данных состояния системы копия файлов реестра компьютера хранится в папке %systemroot%\Repair\Regback. **Если** файлы реестра были повреждены или ошибочно удалены, файлы из этой папки помогут восстановить реестр без полного восстановления данных о состоянии системы. Этот способ рекомендован только опытным пользователям (из Recovery Console).

Создание диска аварийного восстановления

При создании ERD из папки %systemroot%\Repair на дискету копируются файлы:

Имя файла	Описание
Autoexec.nt	Копия файла %systemroot%\System32\Autoexec.nt для инициализации окружения MS-DOS.
Config.nt	Копия файла %systemroot%\System32\Config.nt для инициализации окружения MS-DOS.
Setup.log	Журнал со списком установленных файлов и вычисленных контрольных сумм, используемых в процессе аварийного восстановления. Этот файл имеет атрибуты «только чтение», «системный» и «скрытый» и не виден, пока в окне My Computer (Мой компьютер) не задано отображение всех файлов. Для просмотра можно также воспользоваться командами dir /a, dir /as или dir /ah.

ERD создается после установки Windows 2000. После каждого применения пакета обновлений, изменения данных системы, замены драйверов надо повторно создать ***ERD.*** Своевременно создавайте ERD и храните его в безопасном месте.

Аварийное восстановление

Для восстановления системных файлов после старта компьютера с установочного компакт-диска Windows 2000 или установочных дискет используйте подготовленный ERD Для замены поврежденных файлов установочный компакт-диск Windows 2000 потребуется обязательно.

ERD содержит данные о текущей настройке системы. Убедитесь, что у Вас есть ERD для всех установленных на компьютере копий Windows 2000. Никогда не применяйте ERD от другого компьютера.

В начале аварийного восстановления надо выбрать один из следующих параметров.

- **Manual Repair (Ручное восстановление).** Для выбора из списка параметров нажмите клавишу M. Выбирать этот параметр рекомендуется только опытным пользователям или администраторам системы. Вы восстановите системные файлы, решите проблемы с загрузочным сектором и проанализируете среду загрузки.
- **Fast Repair (Быстрое восстановление).** Для выполнения всех операций восстановления нажмите клавишу F. Это самый простой способ проведения аварийного восстановления — больше пользователю ничего вводить не нужно. После выбора этого параметра процесс аварийного восстановления попытается решить проблемы, связанные с системными файлами, загрузочным сектором на системном диске и средой загрузки (если на компьютере установлено несколько ОС). Файлы реестра будут проверены и восста-

новлены с перезагрузкой каждого раздела реестра. Если раздел не был восстановлен, он будет автоматически скопирован из каталога восстановления в папку %systemroot%\System32\Config.

При выборе Manual Repair файлы реестра не проверяются. При выборе Fast Repair и если доступна папка %systemroot%\Repair, файлы реестра проверяются. Если папка %systemroot%\Repair недоступна, например при повреждении файловой системы, файлы реестра не проверяются.

В режиме Manual Repair можно выбрать один из параметров.

- **Inspect Startup Environment (Анализ среды загрузки).** Проверка начального окружения на правильность файлов Windows 2000 в системном разделе. Отсутствующие или поврежденные файлы будут скопированы с установочного компакт-диска Windows 2000. включая файлы Ntldr и Ntdetect.com. Отсутствующий файл Boot.ini будет создан заново.
- **Verify Windows 2000 System Files (Проверка системных файлов Windows 2000).** Проверка системных файлов Windows 2000 с использованием контрольных сумм и сравнение их с файлами с установочного компакт-диска Windows 2000. Если обнаруживается несовпадение файла, появляется сообщение с именем поврежденного файла и предложением его замены. В процессе восстановления проверяются также наличие и целостность загрузочных файлов, таких как Ntldr и Ntoskrnl.exe.
- **Inspect Boot Sector (Анализ загрузочного сектора).** Проверяет, что загрузочный сектор на системном разделе ссылается на Ntldr. Процесс аварийного восстановления может только заменить загрузочный сектор на системном разделе первого жесткого диска и восстановить загрузочный сектор на системном разделе загрузочного диска.

Примечание При заражении загрузочного сектора вирусом загрузите компьютер с антивирусной загрузочной дискеты. Для проверки и лечения загрузочного сектора следуйте инструкциям антивирусной программы. Одна из них находится на установочном компакт-диске Windows 2000 в папке \3RDPARTY\CA_ANTIV. В прилагаемый к данному курсу компакт-диск эта программа не включена.

Если аварийное восстановление не помогло исправить ошибки

Последняя надежда — повторная установка ОС поверх существующей. Если и это не поможет, потребуется полная переустановка ОС. Затрачиваемое время и в том, и в другом случае одинаково.

Примечание При обновлении установки Windows 2000 возможна потеря пользовательских параметров.

Восстановление данных

Цель всех операций резервного копирования — возможность восстановления поврежденных или утерянных данных. Успешность этой операции гарантируется соблюдением ряда правил. Так, надо документировать все операции резервного копирования, правильно выбирать архивируемые наборы данных, файлы и папки. Кроме того, Вы можете задавать дополнительные параметры в зависимости от Ваших требований к восстановлению информации. В утилите Backup для этого предусмотрен мастер, хотя восстановить данные можно и без него.

Подготовка к восстановлению данных

- Выбирайте стратегию восстановления, основываясь на используемом типе архива. Если время ограничено, используйте комбинацию обычных и разностных архивов — ведь тогда требуется восстановить лишь последнюю обычную и разностную копии.
- Для проверки правильности резервной копии периодически выполняйте тестовое восстановление данных. Оно может вскрыть аппаратные проблемы, которые не проявлялись при проверках при создании резервных копий. Выполняйте тестовое восстановление в другую папку и сравнивайте восстановленные данные с текущими.
- Документируйте архивацию. Для каждого задания создавайте и распечатывайте подробный журнал. Он поможет быстро найти место хранения нужных файлов без загрузки каталогов. *Каталог* (catalog) — это индекс файлов и папок, создаваемый при резервном копировании и хранящийся с соответствующим заданием архивации.
- Делайте записи о заданиях резервного копирования в календарном формате с указанием даты выполнения задания. Для каждого задания указывайте тип архива и имя использованного носителя, например номер ленты или имя съемного диска. Тогда Вы сможете легко выбрать нужную архивную копию среди данных за несколько недель.

Выбор сохраненных наборов данных, файлов и палок для восстановления

Первым делом надо выбрать, какие данные восстанавливать. Вы можете выбрать отдельные файлы и папки, все задание целиком, или *архивный набор* (backup set), — подборку файлов или папок с одного тома, резервную копию которых Вы сделали при копировании. Если Вы делали архив 2 томов, в задании будут 2 архивных набора. Выбрать информацию для восстановления Вы можете, используя каталог.

Восстановить информацию поможет мастер Restore, вызываемый из утилиты Backup. Окно завершения работы мастера отразит начальные значения параметров процесса восстановления. В этот момент можно:

- щелкнуть кнопку Finish (Готово), чтобы закончить восстановление данных; мастер Restore проверит источник данных и выполнит восстановление, а в окне мастера Вы увидите информацию о ходе восстановления;
- задать дополнительные параметры восстановления, щелкнув кнопку Advanced (Дополнительно).

Задание дополнительных параметров восстановления

Зависит от типа используемого при резервном копировании носителя. По окончании работы мастера Restore утилита Backup:

- предлагает проверить правильность выбора носителя, с которого будут восстанавливаться данные; после проверки запускает процесс восстановления данных;
- отображает информацию о состоянии процесса восстановления; как и при резервном копировании, можно просмотреть журнал, содержащий сведения о количестве восстановленных файлов и длительности восстановления.

Ниже описаны дополнительные параметры восстановления.

Параметр	Описание
Restore Files To (Восстановить файлы в)	Место, куда будет восстановлена информация. Можно выбрать один из параметров: Original Location (Исходное размещение) — замена поврежденных или потерянных данных; Alternate Location (Альтернативное размещение) — восстановление более старых версий файлов или пробное восстановление; Single Folder (Единственную папку) — собирает файлы из древовидной структуры в одну папку; задайте этот параметр для копирования отдельных файлов без восстановления иерархической структуры папок, в которых они хранились; при выборе Alternate Location или Single Folder надо указать путь.
When Restoring A File That Is Already On My Computer (Если восстанавливаемый файл уже существует)	Задает перезапись существующих файлов. Можно выбрать один из вариантов: Do Not Replace The File On My Disk (Recommended) (Не заменять имеющийся на диске файл) — предотвращает ошибочную перезапись данных (по умолчанию); Replace The File On My Disk Only If The File On Disk Is Older Than The Backup Copy (Заменять файл на диске, только если он старее архивной копии) — проверяет наличие на компьютере самых свежих версий файлов; Always Replace The File On My Computer (Всегда заменять имеющийся на диске файл) — при совпадении имен файлы из архивной копии заменяют текущие файлы без выдачи запроса.
Advanced Restore Options (Дополнительные параметры восстановления)	Задает восстановление разрешений файлов и специальных системных файлов. Можно выбрать один из параметров: Restore Security (Восстановление безопасности) — устанавливает исходные разрешения файлов, восстанавливаемых на том NTFS: доступа, аудита и атрибуты владения; параметр доступен только при восстановлении копии с тома NTFS на том NTFS; Restore Removable Storage Database (Восстановление базы данных съемных носителей) - восстанавливает конфигурационную БД для съемных носителей и параметры пулов носителей; БД находится в папке %systemroot%\system32\remotestorage; Restore Junction Points, And Restore File And Folder Data Under Junction Points To The Original Location (Восстановление точек соединения, а не папок и файлов, на которые они ссылаются) — восстанавливает точки соединения; выберите этот параметр, если имеется несколько подсоединенных устройств и Вы хотите восстановить данные, на которые они указывают; в противном случае точка восстановится, но данные, на которые она ссылается, будут недоступны.

Упражнение 2: восстановление данных

Вы удалите папку Inetpub, а затем восстановите ее. Выполните упражнение на компьютере Server01.

▶ Задание 1: удалите важные данные

Вы преднамеренно удалите файл Boot.ini. Обычно удаление системных файлов происходит ошибочно или в результате сбоя аппаратуры.

1. Щелкните дважды значок My Computer (Мой компьютер), а затем — Local Disk (C:) [Локальный диск (C:)].

   Откроется одноименное окно.
2. Разверните окно на весь экран.
3. В меню Tools (Сервис) выберите команду Folder Options (Свойства папки).

   Откроется одноименное окно,
4. Перейдите на вкладку View (Вид).
5. Сбросьте флажок Hide Protected Operating System Files (Recommended) (Скрывать защищенные системные файлы).
6. В окне сообщения щелкните кнопку Yes (Да).
7. В окне Folder Options щелкните кнопку OK.

   Количество отображаемых в окне Local Disk (C:) файлов увеличится.
8. Щелкните файл boot.ini.
9. В меню File (Файл) выберите команду Delete (Удалить).
10. В окне Confirm File Delete (Подтверждение удаления файла) щелкните кнопку Yes (Да).

    Файл boot.ini будет удален. Хотя его еще можно восстановить из корзины, мы помним, что в упражнении] была сделана резервная копия этого файла. На следующем этапе используем программу восстановления данных.

▶ Задание 2: восстановление данных

Вы восстановите файл Boot.ini из архивного набора.

1. В окне Local Disk (C:) дважды щелкните файл Backupl.bkf.

   Откроется диалоговое окно Backup — [Untitled] (Архивация — [Безымянный]).
2. Щелкните кнопку Restore Wizard (Мастер восстановления).

   Откроется окно Welcome To The Restore Wizard (Мастер восстановления).
3. Щелкните кнопку Next (Далее).

   Откроется окно What To Restore (Что следует восстановить), где Вам предлагается выбрать носитель архива, с которого будут восстановлены файлы. Заметьте: в данном случае Вам доступен один тип носителя информации — файл и что файлы архивов отсортированы по именам.
4. В окне What To Restore раскройте узел первого задания архивации, созданного в упражнении 1.

   Заметьте: первой папкой в файле резервной копии является диск C: Утилита Backup создает отдельные архивные наборы для каждого сохраняемого тома. Все файлы и папки с одного и того же устройства обозначаются соответствующей тому буквой.
5. Раскройте узел диска C.

   Откроется диалоговое окно Backup File Name (Имя архивного набора), В поле Catalog Backup File (Каталогизировать архивный файл) будет выведено C:\Backupl.bkf. Если там будет текст C:\Backup2.bkf, измените имя на C:\Backupl.bkf.
6. Щелкните кнопку OK.
7. После возврата в окно What To Restore (Что следует восстановить) щелкните C:.

   В колонке Name (Имя) появится файл Boot.ini.
8. Пометьте флажком Boot.ini и щелкните кнопку Next (Далее).

   Откроется окно Completing The Restore Wizard (Завершение работы мастера восстановления).
9. Щелкните кнопку Advanced (Дополнительно).

Откроется окно Where To Restore (Выбор места для восстановления), где предлагается ввести путь для восстанавливаемых файлов.

10. Для просмотра параметров восстановления щелкните раскрывающийся список,
11. Проверьте правильность выбора пути для восстановления файла и щелкните кнопку Next (Далее).
12. Откроется окно How To Restore (Способ восстановления), где назначается порядок восстановления файлов с одинаковыми именами.
13. Проверьте, что выбран параметр Do Not Replace The File On My Disk (Не заменять имеющийся на диске файл) и щелкните кнопку Next (Далее).
14. Откроется окно Advanced Restore Options (Дополнительные параметры восстановления), где для задания резервного копирования выбирают параметры безопасности.
15. Убедитесь, что помечен флажок Restore Security (Восстановление безопасности), сбросьте флажок Restore Junction Points, Not The Folders And File Data They Reference (Восстановление точек соединения, а не папок и файлов, на которые они ссылаются) и щелкните кнопку Next (Далее).

    Откроется окно Completing The Restore Wizard (Завершение работы мастера восстановления), отображающее сводку выбранных Вами параметров.
16. Для начала восстановления файлов щелкните кнопку Finish (Готово).

    Откроется диалоговое окно Enter Backup File Name (Ввод имени архивного файла), где при необходимости указывают имя архивного файла, содержащего восстанавливаемые файлы и папки.
17. Убедитесь, что в поле Restore From Backup File (Восстанавливать из архивного файла) введено C:\Backupl.bkf, и щелкните кнопку OK.

    Откроется диалоговое окно Restore Progress (Ход восстановления), где отображается информация о состоянии задания резервного копирования, примерном суммарном размере и текущем размере обработанных данных, текущем времени выполнения задания и времени, оставшемся до его завершения.
18. По завершении восстановления щелкните кнопку Report (Отчет).

    Запустится программа Notepad со сформированным отчетом о восстановлении. В журнал резервного копирования добавятся подробные сведения о произведенном восстановлении. В журнале централизованно хранится вся информация об операциях резервного копирования и восстановления.
19. После просмотра отчета закройте программу Notepad.
20. В диалоговом окне Restore Progress (Ход восстановления) щелкните кнопку Close (Закрыть).
21. Закройте диалоговое Backup — [Untitled].

    Откроется окно Local Disk (C:).
22. Удостоверьтесь, что файл Boot.ini был успешно восстановлен.
23. Закройте окно Local Disk (C:).

Восстановление томов RAID-1 и RAID-5

Мы обсудим восстановление данных в случае повреждения одного из зеркальных томов или томов RAID-5.

Восстановление информации с поврежденного зеркального тома

Компьютер сохраняет информацию на каждом диске **зеркального** тома **одновременно. Если один из них** отказывает, **другой** продолжает **нормально работать.**

Поврежденный диск надо сначала **исключить из зеркального тома** через **оснастку Computer** Management (Управление **компьютером), а затем заменить на** исправный.

Для повторного создания зеркального тома после замены поврежденного диска щелкните правой кнопкой рабочий раздел в окне Computer Management и выберите в контекстном меню команду Add Mirror (Добавить зеркало). На рис. 12-14 диск D на диске О имеет зеркальную копию на диске 1.

Рис. 12-14. Замена поврежденного диска из состава зеркального тома

Если поврежден главный диск зеркального тома, включая загрузочный раздел, для запуска компьютера и доступа к работающему диску тома используйте загрузочный диск. Файл Boot.ini на загрузочном диске должен содержать ARC-путь, указывающий на зеркальный раздел. Рекомендуется тестировать загрузочный диск сразу после создания зеркального тома.

Примечание Зеркальный том удаляют не только в случае отказа одного из его дисков, но и для использования дискового пространства в других целях.

Восстановление тома RAID-5

При отказе одного диска тома RAID-5 доступ ко всем данным тома сохраняется. Драйвер отказоустойчивости Windows 2000 Server использует для восстановления отсутствующих данных в оперативной памяти данные и контрольные суммы с оставшихся дисков. При восстановлении данных производительность компьютера снижается.

Для восстановления нормального уровня производительности надо заменить поврежденный диск и восстановить том RAID-5. Драйвер отказоустойчивости на основе контрольных сумм, хранящихся на работающих дисках, заново создает данные поврежденного диска и переписывает их на новый исправный диск.

Резюме

Аварийное восстановление позволяет войти в систему и получить доступ к ресурсам системы после сбоя. В Windows 2000 предусмотрено три способа восстановления работоспособности системы: безопасный режим, Recovery Console и ERD. В безопасном режиме система запускается с минимальным набором драйверов устройств и служб. Текстовый интерпретатор команд Recovery Console, отличный от командной строки Windows 2000, позволяет администратору получить доступ к жесткому диску Windows 2000-компьютера. Диск ERD применяется для восстановления основных системных файлов. Наряду с восстановлением работоспособности системы можно восстановить и данные. Утилита Backup предлагает услуги мастера Restore. Вы можете восстановить данные и без мастера. Если в системе установлены отказоустойчивые диски, информацию можно восстановить с зеркального тома или тома RAID-5.

Закрепление материала

? J Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. На Вашем компьютере по умолчанию загружается Windows 2000 Server, но можно загрузить и Windows NT 4.0. После изменения атрибутов файлов в %systemdrive% и удаления некоторых из них компьютер перестал выполнять двухвариантную загрузку. Windows 2000 загружается нормально. Проблема появилась после того, как Вы удалили файл. Как называется этот файл и как исправить эту ошибку?

2. Для своего мобильного компьютера Вы создали три профиля оборудования: Docked (Пристыкован), Undocked On The Network (Отстыкован в сети) и Undocked At Home (Отстыкован дома). После перезагрузки первые два профиля остались, а третий исчез. Назовите наиболее вероятную причину отсутствия профиля Undocked At Home.

3. Почему недоступен флажок Use Hardware Compression, If Available (Использовать аппаратное сжатие, если возможно) в мастере Backup?

4. Вы создали полную резервную копию в понедельник. В оставшиеся дни недели Вы хотите копировать только те файлы и папки, которые изменялись за прошедший день. Какой тип архива выбрать?

5. Как проверить настройку службы UPS?

ГЛАВА 13

Мониторинг и оптимизация

В этой главе

Ряд утилит Microsoft Windows 2000 предназначен для мониторинга и оптимизации производительности системы. Так, программа Disk Defragmenter (Дефрагментация диска) позволяет выявлять в локальных томах и объединять фрагментированные файлы/папки, а Network Monitor — выявлять и определять проблемы сети. В этой главе рассматривается большинство утилит и служб для мониторинга, разрешения проблем и настройки системы, включая средства оптимизации производительности дисков и сети.

Прежде всего

Для изучения материалов этой главы необходимо:

- установить Windows 2000 Server на Server01;
- выполнить упражнения предыдущих глав.

Занятие 1. Мониторинг и оптимизация производительности дисков

Мы обсудим утилиты Windows 2000, предназначенные для диагностики дисков, повышения производительности и сжатия данных: Check Disk, Disk Defragmenter, а также процессы сжатия данных и квотирования дисков. На занятии 2 мониторинг и оптимизация дисков рассмотрены в контексте мониторинга производительности системы.

Изучив материал этого занятия, Вы сможете:

- ✓ оптимизировать производительность дисков с помощью утилиты Check Disk, оснастки Disk Defragmenter, сжатия данных и дисковых квот.

Продолжительность занятия — около 40 минут.

Утилита Check Disk

Check Disk (Проверка диска) позволяет выявить ошибки файловой системы и поврежденные сектора на жестком диске. Для вызова Check Disk откройте окно свойств диска, который надо проверить. Это можно сделать с помошью Windows Explorer или из окна My Computer. На вкладке Tools (Сервис) щелкните кнопку Check Now (Выполнить проверку). В открывшемся окне можно задать параметры проверки (рис. 13-1).

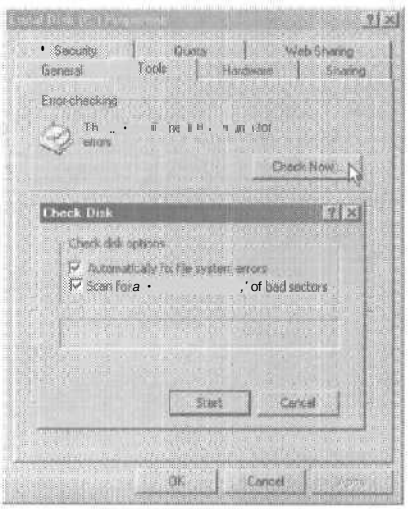


Рис. 13-1. Диалоговое окно Check Disk

Для автоматического исправления ошибок файловой системы перед запуском Check Disk на проверяемом диске надо закрыть все запущенные приложения и открытые файлы. Иначе Вы увидите сообщение о невозможности получить монопольный доступ к диску, и Вам будет предложено выполнить проверку диска при следующем запуске системы. В томах с NTFS Windows 2000 регистрирует все файловые транзакции, автоматически заменяет поврежденные кластеры и сохраняет копии ключевой информации для всех файлов.

Оснастка Disk Defragmenter

Windows 2000 сохраняет файлы/папки в ближайшую свободную область диска, необязательно непрерывную. Это приводит к фрагментации файлов/папок. Если на жестком диске много фрагментированных файлов/папок, время доступа к ним увеличивается, так как сбор нескольких частей файла/папки требует больше операций чтения. Создание новых файлов/папок тоже займет больше времени, поскольку свободное пространство разбросано по всему диску, из-за чего файлы/папки приходится сохранять в разных частях диска.

Дефрагментация дисков

Процесс поиска и объединения фрагментированных файлов/папок называется *дефрагментацией* (defragmenting). Именно для этого предназначена оснастка Disk Defragmenter (Дефрагментация диска), которая переносит части файла/папки в одно место так, что каждый файл/папка занимает одну непрерывную область свободного пространства. Благодаря этому ускоряется доступ и сохранение файлов/папок. При этом Disk Defragmenter «объединяет» свободное место, что снижает вероятность фрагментации новых файлов. Оснастка Disk Defragmenter работает с томами FAT16, FAT32 и NTFS.

Запустить Disk Defragmenter можно из оснастки Computer Management (Управление компьютером) или создав для этого пользовательскую консоль. Кроме того, Disk Defragmenter запускается из диалогового окна свойств диска, открываемого с помощью Windows Explorer или из окна My Computer (рис. 13-2). На вкладке Tools (Сервис) шелкните кнопку Defragment Now (Выполнить дефрагментацию).

В верхней части окна показаны тома, которые можно анализировать и дефрагментировать, в нижней — диаграмма фрагментации выбранного тома и динамическая диаграмма тома, обновляемая при дефрагментации. Для иллюстрации состояния тома используются такие цвета:

- красный — фрагментированные файлы;
- темно-синий — непрерывные файлы;
- белый — свободное пространство;
- зеленый — системные файлы, которые Disk Defragmenter не может перемещать.

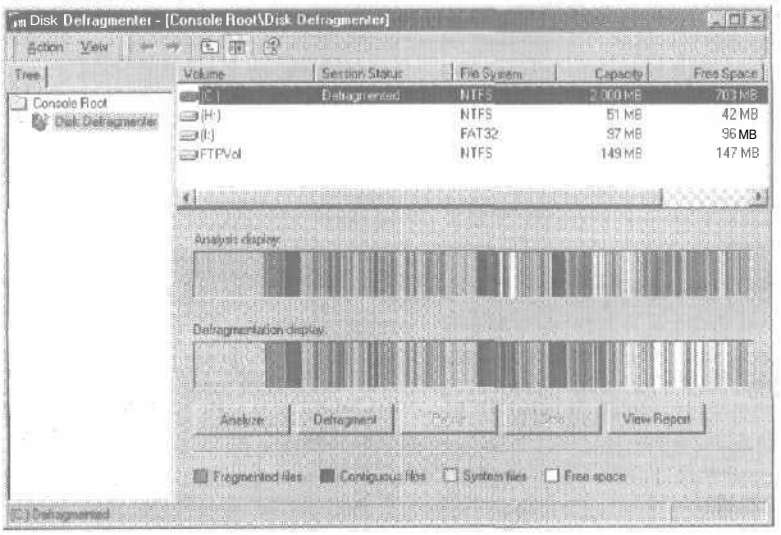


Рис. 13-2. Оснастка Disk Defragmenter, запущенная из пользовательской консоли

Сравнив диаграммы в процессе и по завершении дефрагментации, Вы сразу же увидите улучшения в размещении файлов в данном томе.

Для анализа или дефрагментации тома щелкните одну из кнопок:

Кнопка	Описание
Analyze (Анализ)	Анализ состояния диска. По завершении анализа на верхней диаграмме отражается степень фрагментации тома.
Defragment (Дефрагментация)	Дефрагментация диска. По завершении дефрагментации нижняя диаграмма покажет состояние дефрагментированного тома.

Рекомендации по работе с Disk Defragmenter

- Запускайте Disk Defragmenter в периоды наименьшей загруженности системы. В процессе дефрагментации данные перемещаются из одних областей жесткого диска в другие. При дефрагментации интенсивно используется процессор, что заметно замедляет доступ к дисковым ресурсам.
- Рекомендуйте пользователям дефрагментировать локальные жесткие диски не реже одного раза в месяц.
- Перед установкой больших приложений проанализируйте и при необходимости дефрагментируйте конечный том. Если на конечном носителе хватает непрерывного свободного пространства, установка проходит быстрее. Кроме того, ускоряется доступ к установленному приложению,
- После удаления большого числа файлов/папок проанализируйте состояние жесткого диска. На интенсивно работающих файловых серверах дефрагментацию дисков надо выполнять чаще, чем на компьютерах, используемых одним клиентом.
- Рассмотрите возможность использования утилиты для дефрагментации дисков, позволяющей регулярно, по расписанию, дефрагментировать все сетевые диски. Компания Executive Software, разработавшая утилиту Disk Defragmenter для Windows 2000, предлагает автоматизированную версию данной программы (Diskeeper) с расширенными возможностями, поставляемую отдельно.

Примечание Подробности о программе Diskeeper 5.0 производства Executive Software см. по адресу *http://www.exesoft.com*.

Сжатие данных

Средства сжатия файлов и папок в томах NTFS позволяют экономить место. Каждый файл/папка в томе NTFS может быть в состоянии «сжат(а)» или «не сжат(а)».

Работа со сжатыми файлами и папками

Чтение и запись сжатых файлов Windows- и MS-DOS-приложениями не требует их предварительного разуплотнения. Когда приложение или команда ОС формирует запрос на доступ к сжатому файлу, NFTS автоматически его разуплотняет. При закрытии или явном сохранении файла NTFS снова сжимает его.

NTFS выделяет дисковое пространство, основываясь на размере разуплотненного файла. При копировании сжатого файла в том NTFS, где для сжатого файла место есть, а для разуплотненного не хватает, появится соответствующее сообщение, и файл копироваться не будет.

Сжатие файлов и папок

Определить состояние сжатия файла/папки позволяют Windows Explorer и утилита compact. Информацию о синтаксисе этой утилиты Вы получите, набрав в командной строке **compact /?.**

Для сжатия откройте окно свойств файла/папки. На вкладке General (Общие) щелкните кнопку Advanced (Другие). В диалоговом окне Advanced Attributes (Дополнительные атрибуты) пометьте флажок Compress Contents to Save Disk Space (Сжимать содержимое для экономии места на диске) (рис. 13-3). Учтите, что шифрование NTFS и сжатие данных — взаимоисключающие возможности, поэтому при помеченном флажке Encrypt Contents To Secure Data (Шифровать содержимое для зашиты данных) сжатие применить нельзя.

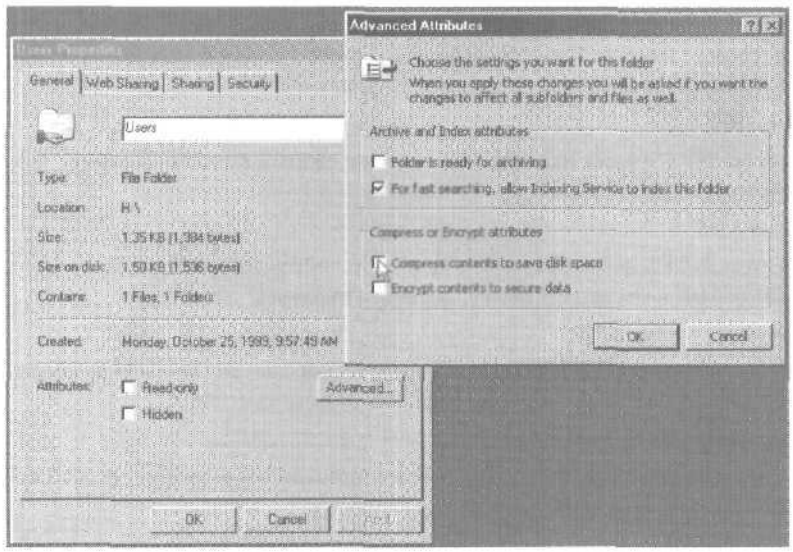


Рис. 13-3. Диалоговое окно Advanced Attributes (Дополнительные атрибуты)

Диск можно сжать целиком. Для этого на вкладке General диалогового окна свойств диска пометьте флажок Compress Drive To Save Disk Space (Сжимать диск для экономии места). Чтобы изменить состояние сжатия файла/папки, необходимо иметь разрешение Write. Флажок сжатия папки не отражает состояния сжатия находящихся в ней данных и вложенных в нее папок/файлов. Папку можно настроить так, что добавляемые в нее файлы будут сжиматься, а хранящиеся останутся несжатыми. Возможно и обратное: папка без флажка сжатия может содержать сжатые файлы. После того, как Вы выберете параметры сжатия папки и щелкнете в диалоговом окне свойств кнопку OK или Apply (Применить), Windows 2000 выведет диалоговое окно Confirm Attribute Changes (Подтверждение изменения атрибутов), содержащее два дополнительных параметра:

Параметр	Описание
Apply changes to this folder only (Только к этой папке)	Сжимаются только файлы в выбранной папке.
Apply changes to this folder, subfolders and files added to it (К этой папке и ко всем вложенным файлам и папкам)	Сжимаются файлы в выбранной папке; для вложенных папок помечается флажок сжатия; сжимаются как имеющиеся, так и добавляемые позже файлы.

Внимание! Windows 2000 не поддерживает сжатие для кластеров объемом более 4 Кб, так как сжатие в томах с большими кластерами приводит к падению производительности. Если при форматировании тома NTFS указать размер кластера более 4 Кб, сжать данные в этом томе будет нельзя.

Выделение сжатых файлов и папок цветом

Для отображения сжатых файлов/папок можно использовать разные цвета. Для этого выберите в меню Tools (Сервис) команду Folder Options (Свойства папки) и на вкладке View (Вид) пометьте флажок Display Compressed Files And Folders With Alternate Color (Отображать сжатые файлы и папки другим цветом).

Копирование и перемещение сжатых файлов и папок

Существуют правила, определяющие наследование состояния сжатия файлов/папок при их копировании или перемещении между разделами FAT или NTFS.

Копирование файла в томе NTFS

При копировании в томе NTFS файл наследует состояние сжатия конечной папки. Так, сжатый файл, копируемый в несжатую папку, автоматически разуплотняется.

Перемещение файла в томе NTFS

При перемещении в томе NTFS файл сохраняет исходное состояние сжатия. Например, сжатый файл, перемещаемый в несжатую папку, остается таковым.

Копирование файла/папки между томами NTFS

При копировании между томами NTFS файл/папка наследует состояние сжатия конечной папки.

Перемещение файла/папки между томами NTFS

Поскольку Windows 2000 выполняет перемещение как копирование и удаление, файл/папка наследует состояние сжатия конечной папки.

Перемещение файла/папки в том FAT

Так как Windows 2000 поддерживает сжатие только файлов NTFS, при копировании сжатого файла/папки NTFS в раздел FAT этот файл/папка автоматически разуплотняется.

Перемещение или копирование сжатого файла/папки на гибкий диск

При перемещении или копировании сжатого файла/папки NTFS на гибкий диск соответствующий файл/папка автоматически разуплотняется.

Примечание При копировании сжатого файла NTFS Windows 2000 разуплотняет и копирует его и, если для конечной папки установлен флажок сжатия, снова сжимает файл. Это может привести к падению производительности.

Рекомендации по использованию сжатия NTFS

- Поскольку файлы некоторых типов сжимаются сильнее, чем файлы других типов, при сжатии рекомендуется руководствоваться их конечным размером. Так, растровые изображения Windows, которые по сравнению с исполняемыми файлами содержат больше избыточных данных, при сжатии займут меньше места. Растровые изображения обычно сжимаются до 25% от исходного размера, а исполняемые файлы — до 75%.

- В сжатой папке не рекомендуется хранить заархивированные файлы, например файлы PKZIP. Windows 2000 попытается сжать архив, что приведет к напрасным тратам системного времени и не даст выигрыша в дисковом пространстве.
- Чтобы упростить поиск сжатых данных, для отображения сжатых файлов/папок используйте обозначение цветом.
- Рекомендуется сжимать статичные, а не динамически изменяющиеся данные. Сжатие/разуплотнение файлов загружает процессор. Сжимая файлы, к которым редко обращаются, Вы ускоряете работу системы.
- Сжатие NTFS несколько снизит производительность при копировании и перемещении файлов. Сжатый файл, копируемый в папку с флажком сжатия, разуплотняется, копируется и вновь сжимается.

Дисковые квоты

Вы можете выделять пользователям дисковое пространство, основываясь на принадлежащих им файлах/папках. Дисковые квоты и их пределы можно устанавливать как для отдельных, так и для всех пользователей. Кроме того, Вы можете осуществлять мониторинг занятого пользователем дискового объема и оставшегося пространства квоты.

Управление дисковыми квотами

Windows 2000 отслеживает дисковые квоты для каждого тома, даже если тома находятся на одном жестком диске. Контроль занимаемого пользователем дискового объема осуществляется независимо от папки, в которой хранятся файлы. Утилиты сторонних фирм позволяют получать более подробную информацию о занятости дискового пространства.

Важные характеристики дисковых квот Windows 2000 таковы.

- Windows 2000 определяет объем занятого пространства, основываясь на принадлежащих пользователю файлах/папках. Когда пользователь копирует или сохраняет новый файл в том NTFS или становится владельцем файла в томе NTFS, Windows 2000 сравнивает объем пространства, необходимый для размещения файла, и квоту пользователя.
- При определении объема занятого пространства Windows 2000 игнорирует сжатие. Учитывается каждый несжатый байт независимо от того, сколько места на самом деле занимают файлы/папки пользователя. Отчасти такой учет осуществляется из-за того, что степени сжатия файлов разных типов не одинаковы. В развернутом виде файлы разных типов могут быть одного объема, но при сжатии их размеры могут сильно различаться.
- Если используются дисковые квоты, свободное пространство на диске, предоставляемый приложениям Windows 2000, будет равно оставшемуся пространству квоты пользователя. Допустим, файлы занимают 50 Мб из назначенной квоты в 100 Мб — Windows 2000 покажет, что объем свободного места на диске равен 50 Мб, даже если том содержит несколько гигабайт незанятого пространства.

Примечание Дисковые квоты можно использовать только в томах Windows 2000 NTFS.

Дисковые квоты позволяют осуществлять мониторинг и управлять использованием пространства диска. Администраторы могут:

- устанавливать дисковую квоту для каждого пользователя;
- задавать порог выдачи предупреждений, при достижении которого Windows 2000 отмечает в журнале событие, указывающее на то, что пользователь почти достиг предела своей дисковой квоты;

- обеспечивать соблюдение пределов дисковых квот и блокировать или не блокировать доступ при превышении квоты;
- регистрировать событие, означающее, что дисковое пространство, занимаемое пользователем, достигло пороговой величины, например, при превышении квоты или порога выдачи предупреждения.

После того как Вы включите дисковые квоты, Windows 2000 соберет для всех пользователей, файлы/папки которых размещаются в этом томе, сведения о занимаемом дисковом пространстве, что позволит Вам осуществлять мониторинг тома для каждого пользователя. Просматривать и изменять параметры дисковых квот по умолчанию могут лишь члены группы Administrators, Систему можно настроить, чтобы пользователи могли просматривать параметры квот.

Включение дисковых квот

Дисковые квоты и пороги выдачи предупреждения можно включить для отдельных или всех пользователей. Дисковые квоты задаются на вкладке Quota (Квота) диалогового окна Properties диска (рис. 13-4).

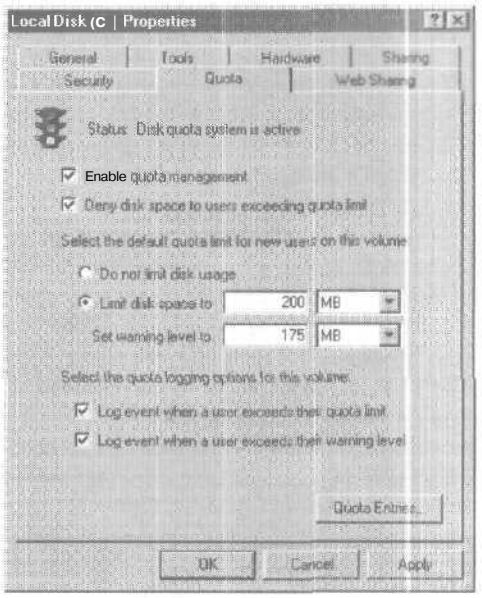


Рис. 13-4. Вкладка Quota (Квота) диалогового окна свойств диска

Параметры вкладки Quota.

Параметр	Описание
Enable Quota Management (Включить управление квотами)	Флажок включает/отключает управление дисковыми квотами.
Deny Disk Space **To Users** Exceeding **Quota** Limit (Не выделять место на диске **при превышении** квоты)	При помеченном флажке пользователи, превысившие квоту, не смогут записывать файлы в том и получат сообщение, что на диске не хватает места.
Do Not Limit Disk Usage **(Не ограничивать** выделение места на диске)	Переключатель снимает ограничения на использование дискового пространства.

(окончание)

Параметр	Описание
Limit Disk Space To (Выделять на диске не более)	Здесь указывается объем дискового пространства, доступного пользователям.
Set Warning Level To (Порог выдачи предупреждений)	Здесь указывается объем дискового пространства, которое может занять пользователь перед тем, как Windows 2000 зарегистрирует событие, сообщающее, что пользователь почти достиг предела своей квоты.
Quota Entries (Записи квот)	Щелчок этой кнопки открывает диалоговое окно Quota Entries For, где можно добавить/удалить запись и узнать о квоте конкретного пользователя.

Чтобы задать одинаковые пределы квот для всех пользователей, введите соответствующие значения в полях Limit Disk Space To (Выделять на диске не более) и Set Warning Level To (Порог выдачи предупреждений) и пометьте флажок Deny Disk Space To Users Exceeding Quota Limit (Не выделять место на диске при превышении квоты). Windows 2000 не позволит создавать в томе папки/файлы пользователям, превысившим квоту.

Определение состояния дисковых квот

Чтобы определить состояние дисковых квот, в диалоговом окне Properties диска просмотрите сообщение справа от значка светофора (рис. 13-4). Цвета светофора означают:

- красный — дисковые квоты не используются;
- желтый — Windows 2000 восстанавливает сведения о дисковых квотах;
- зеленый — система дисковых квот включена.

Соблюдение дисковых квот

Чтобы задать квоты для нескольких пользователей, щелкните кнопку Quota Entries. В появившемся диалоговом окне Quota Entries For (Записи квот для) можно указать предельный объем дискового пространства и порог выдачи предупреждений для каждого пользователя.

Диалоговое окно Quota Entries For *<имя_тома>* позволяет осуществлять мониторинг занимаемого дискового пространства для всех пользователей, которые скопировали, сохранили или владеют файлами/папками в данном томе. Windows 2000 сканирует том и определяет объем дискового пространства, занятого каждым пользователем. Диалоговое окно Quota Entries For *<имя_тома>* позволяет узнать о:

- дисковом пространстве, занимаемом каждым пользователем;
- пользователях, превысивших порог выдачи предупреждений (желтый треугольник);
- пользователях, превысивших квоту (красный кружок);
- пороге выдачи предупреждений и дисковой квоте каждого пользователя.

Обращение к тому отслеживается для всех пользователей, которым принадлежат файлы в томе с включенной системой дисковых квот. Владельцу файлов на данном диске, которому не задана персональная квота в окне Quota Entries For *<имя_тома>*, дисковая квота назначается по умолчанию. Пользователи, у которых в этом томе файлов нет, в окне Quota Entries For *<имя_тома>* не отображаются, но их можно добавить вручную. По умолчанию дисковые квоты не распространяются на членов локальной группы Administrators (Администраторы).

Рекомендации по использованию дисковых квот

- Если в томе, где установлена Windows 2000, включена система дисковых квот и они распространяются на Вашу учетную запись пользователя, то для установки дополнительных приложений и компонентов Windows 2000 Вы должны зарегистрироваться в системе как Administrator. По умолчанию дисковые квоты не распространяются на членов группы Administrators, состояние дисковой квоты Вашей учетной записи пользователя не изменится.
- Осуществлять мониторинг дискового пространства и генерировать соответствующие сведения можно, не блокируя пользователям возможность сохранения данных. Для этого при включении системы дисковых квот сбросьте флажок Deny Disk Space To User Exceeding Quota Limit (Не выделять место на диске при превышении квоты).
- Для начала выделите всем пользователям небольшой объем дискового пространства, а затем в окне Quota Entries For *<имя_тома>* измените параметры квот для тех, кто работает с большими файлами.
- Включайте квоты для общедоступных дисков, чтобы ограничить пространство, занимаемое каждым пользователем. Задавайте квоты для общедоступных папок и сетевых серверов — это позволит гарантировать равномерное использование пространства. При нехватке жестких дисков квоты можно установить для всего разделяемого пространства.
- Записи о квотах пользователей, у которых нет файлов в томе, следует удалять.
- Запись о квоте можно удалитьлишь после того, как все файлы, принадлежащие пользователю, будут удалены из тома или будут переданы во владение другому пользователю. Эффективный способ удалить файлы пользователя или передать их во владение себе — удалить запись о квоте в диалоговом окне Quota Entries For *<имя_тома>*. Система управления дисковыми квотами выведет диалоговое окно, позволяющие переместить, удалить или вступить во владение файлами.

Упражнение 1: включение дисковых квот

Измените используемые по умолчанию параметры управления дисковыми квотами и ограничьте объем информации, которую пользователи могут хранить на диске C: компьютера Server01. На диске C: имеется разделяемый общедоступный каталог HomeDirs, созданный Вами для John Smith. Затем настройте для пользователя персональную дисковую квоту — увеличьте максимальный объем дискового пространства, доступный пользователю, до 20 Мб, и установите порог выдачи предупреждений равным 16 Мб. После этого отключите управление квотами для диска C:. Упражнение выполняйте на ServerOl.

▶ Задание 1: настройте параметры управления квотами

Настройте параметры управления квотами для диска C: и ограничьте объем информации, которую пользователи могут хранить в томе.

1. Зарегистрируйтесь на ServerOl как Administrator (Администратор) с паролем password.
2. Дважды щелкните значок My Computer (Мой компьютер).
3. Щелкните значок Local Disk (C:) [Локальный диск (C:)], затем в меню File (Файл) выберите команду Properties (Свойства).

   Откроется диалоговое окно свойств локального диска C:.
4. Перейдите на вкладку Quota (Квота).

   Заметьте: по умолчанию дисковые квоты отключены.
5. Пометьте флажок Enable Quota Management (Включить управление квотами).

6. Щелкните переключатель Limit Disk Space To (Выделять на диске не более).
7. В списке рядом с этим полем введите 10, а в поле Set Warning Level To (Порог выдачи предупреждений) — 6.

   Заметьте: по умолчанию размер указывается в килобайтах.
8. Измените единицу измерения на мегабайт и щелкните кнопку Apply (Применить).

   Откроется диалоговое окно Disk Quota (Дисковая квота), предупреждающее, что при включении дисковых квот в целях обновления статистики об использовании дискового пространства будет произведено сканирование тома.
9. Щелкните кнопку OK, чтобы включить дисковые квоты.
10. Не закрывайте окно свойств диска — оно Вам понадобится.

► Задание 2: настройте персональную дисковую квоту для пользователя

Настройте для пользователя John Smith персональную дисковую квоту.

1. На вкладке Quota (Квота) диалогового окна свойств диска C: щелкните кнопку Quota Entries (Записи квот).

   Откроется диалоговое окно Quota Entries For Local Disk (C:) [Записей квот для Локальный диск (C:)]. Обратите внимание, что в окне перечислены созданные Вами учетные записи пользователей, группы NT AUTHORITY\SYSTEM и BUILTIN\Administrators (BUILTIN\Администраторы). Учетные записи (Jane_Doe, Jonh_ Smith и Bob_Train) перечислены потому, что соответствующим пользователям принадлежат файлы на диске C:.
2. Дважды щелкните запись John Smith.

   Откроется диалоговое окно Quota Settings For John Smith (Параметры квоты для John Smith).
3. Введите в поле Limit Disk Space To (Выделять на диске не более) 20, а в поле Set Warning Level To (Порог выдачи предупреждений) — 16.
4. Щелкните кнопку OK, чтобы вернуться к диалоговому окну Quota Entries For Local Disk (C:) [Записей квот для Локальный диск (C:)].
5. Закройте диалоговое окно Quota Entries For Local Disk (C:).
6. Не закрывайте окно свойств диска — оно Вам понадобится.

► Задание 3: отключите управление дисковыми квотами

Отключите управление дисковыми квотами для диска C:.

1. На вкладке Quota (Квота) сбросьте флажок Enable Quota Management (Включить управление квотами).

   Параметры квот для диска C: станут недоступны,
2. Щелкните кнопку Apply (Применить).

   Диалоговое окно Disk Quota (Дисковая квота) предупредит, что при повторной активации системы дисковых квот будет произведено сканирование тома.
3. Щелкните кнопку OK, чтобы закрыть диалоговое окно Disk Quota.
4. Щелкните кнопку OK, чтобы закрыть диалоговое окно Local Disk (C:) Properties.
5. Закройте окно My Computer (Мой компьютер).

Резюме

В Windows 2000 имеется несколько средств диагностики проблем дисков, повышения производительности путем сжатия данных. Утилита Check Disk (Проверка диска) позволяет выявлять ошибки файловой системы и поврежденные секторы диска. Оснастка Disk Defragmenter (Дефрагментация диска) позволяет выявлять и дефрагментировать файлы/папки, части которых переносятся в одно место, чтобы файл/папка занимал одну последовательную область дискового пространства. Сжатие данных позволяет сжимать файлы/папки в томах NTFS. Любые приложения для Windows и MS-DOS могут считывать и записывать сжатые файлы без их предварительного разуплотнения другой программой. Дисковые квоты позволяют ограничивать доступное пользователям дисковое пространство, а также отслеживают и контролируют его использование для каждого тома и для каждого пользователя.

Занятие 2. Служба SNMP

Для разработки эффективной платформы управления разнородными сетями TCP/IP в 1988 г. был создан протокол SNMP (Simple Network Management Protocol). В 1990 г. он был утвержден группой IAB (Internet Activities Board) как стандарт Интернета. SNMP позволяет осуществлять мониторинг и передавать *станции управления сетью* (network management station, NMS) сведения о состоянии от агентов SNMP. На этом занятии обсуждаются вопросы внедрения SNMP в Windows 2000.

Изучив материал этого занятия, Вы сможете:

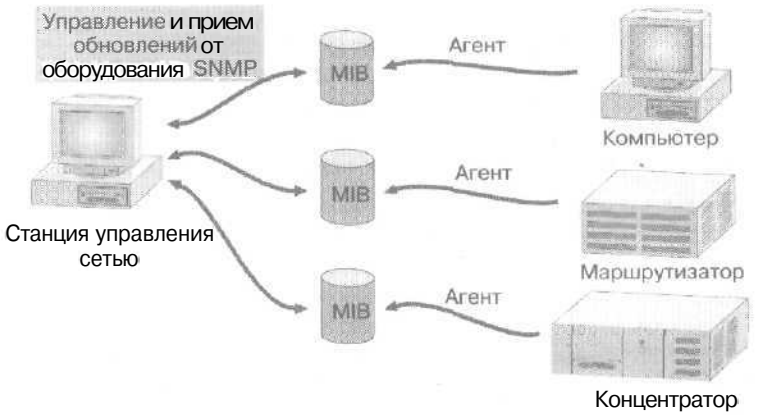
- ✓ описать назначение и принцип работы службы SNMP.

Продолжительность занятия — около 35 минут.

Обзор SNMP

SNMP — стандарт управления сетью, широко используемый в сетях TCP/IP и IPX, позволяющий централизованно контролировать узлы сети (серверы, рабочие станции, маршрутизаторы, мосты и концентраторы) со станции управления сетью.

Для осуществления функций управления SNMP использует распределенную архитектуру систем и агентов управления (рис. 13-5). Центральный узел (хост), на котором выполняется ПО управления сетью, называется станцией управления сетью или диспетчером SNMP. Управляемые узлы называются агентами SNMP.



Рис, 13-5. Распределенная архитектура SNMP

Атент передает в *базу данных управляющей информации* (Management Information Base, MIB) информацию о конфигурации и состоянии оборудования. MIB определяет, какие сведения об оборудовании и ПО надо собрать на хосте. Для реализации функций по мониторингу устройств агент SNMP взаимодействует с NMS.

SNMP используется для:

- **конфигурирования удаленных устройств** — можно определить сведения, которые будут отсылаться станцией управления сетью каждому хосту сети;
- **мониторинга производительности** сети — можно отслеживать скорость обработки и пропускную способность сети и собирать информацию об успешности передачи данных;

- **выявления ошибок сети или несанкционированного доступа** — для сетевых устройств можно определить триггеры, срабатывающие при наступлении определенных событий; при этом устройство пересылает NMS сообщение о наступившем событии; сигналы оповещения можно настроить для:
  - останова или перезапуска службы;
  - выявления отказа канала на маршрутизаторе;
  - несанкционированного доступа к узлу сети;
- **аудита использования сети** — можно осуществлять мониторинг общего применения сети для выявления пользователей и групп или видов обращения к сетевым устройствам и службам.

Агент SNMP реализован в Windows 2000 в виде 32-разрядной службы, работающей на компьютерах с протоколами TCP/IP и IPX. В Windows 2000 реализованы версии 1 и 2С протокола SNMP, основанные на промышленных стандартах, определяющих порядок структурирования и хранения данных для управления сетью и порядок передачи их между агентами и системами управления сетями **TCP/IP.**

Для использования информации, предоставляемой службой SNMP, в сети должна быть хотя бы одна NMS. Служба SNMP в Windows 2000 является лишь агентом и не включает управляющего ПО SNMP. Чтобы превратить хост в станцию управления сетью, воспользуйтесь управляющим ПО **SNMP** третьих фирм.

Системы управления и агенты

NMS необязательно должна размещаться на том же компьютере, что и агенты SNMP. NMS может получать от агентов **SNMP:**

- идентификаторы и статистические данные сетевых протоколов;
- динамически назначаемые идентификаторы устройств, подключенных к сети;
- сведения о конфигурации аппаратного и программного обеспечения;
- сведения о производительности и использовании устройств;
- ошибки и сообщения о событиях устройств;
- статистические данные об использовании программ и приложений.

Система управления может отсылать агенту конфигурационную информацию, изменяющую локальные параметры системы, однако на практике это происходит редко, так как большинство параметров клиентов доступны лишь для чтения.

Агенты SNMP предоставляют диспетчерам **SNMP** сведения об операциях, происходящих на сетевом уровне протокола IP, и отвечают на запросы о предоставлении информации, генерируемые NMS. Любой компьютер, на котором выполняется ПО агента **SNMP,** например, служба Windows 2000 SNMP, является агентом SNMP. Вы можете настроить параметры службы агента и определить, какие данные она должна собирать и какие системы их могут запрашивать.

В большинстве случаев агенты не генерируют сообщения, а отвечают на них. Исключением является предупреждающее сообщение — *сообщение ловушки* (trap message). *Ловушка* (trap) — это событие клиентской системы, например перезагрузка или несанкционированный доступ, в случае которого генерируется сообщение. Ловушки обеспечивают элементарную форму безопасности, извещая систему управления о подозрительных событиях.

База данных управляющей информации

MIB (Management Information Base) — это контейнер объектов, представляющих определенный тип информации. MIB содержит необходимые системе управления сведения. Например, один объект MIB может представлять число активных сессий, другой — объем

дискового пространства на клиенте. Все данные, которые система управления может запросить у агента, хранятся в различных **MIB.**

Каждый объект в MIB обладает следующими атрибутами;

- имя и идентификатор;
- тип данных;
- текстовое описание;
- способ индексирования объектов, представляющих сложные данные (обычно многомерного массива или таблицы) — список установленных в системе сетевых интерфейсов, таблица маршрутизации или таблица протокола ARP;
- разрешения доступа.

Каждый объект **MIB** наделен уникальным идентификатором, включающим:

- тип — counter (счетчик), string (строка), gauge (индикатор) или address (адрес);
- уровень доступа — read (чтение) или read/write (чтение/запись);
- ограничения размера;
- диапазон.

Служба Windows 2000 **SNMP** поддерживает Internet MIB II, LAN Manager MIB II, Host Resources MIB, а также MIB, разработанные Microsoft, такие как WINS MIB, DHCP MIB и IIS MIB.

Сообщения SNMP

Агенты и системы управления **SNMP** исследуют и обмениваются информацией об управляемых объектах с помощью сообщений SNMP, которые пересылаются по протоколу UDP (User Datagram Protocol). Для маршрутизации сообщений между NMS и хостом используется протокол IP. По умолчанию на 161 порту UDP перехватываются сообщения SNMP, а на 162 порту — ловушки SNMP.

Когда программы управления SNMP отправляют запросы на сетевое устройство. ПО агента на этом устройстве получает их и извлекает нужные сведения из MIB. Затем агент отправляет запрошенные сведения в исходную программу управления SNMP. Для этого используются следующие сообщения.

- GET — основное запрашивающее сообщение SNMP. Отправляется системой управления SNMP для запроса у агента сведений об одной записи MIB, например об объеме свободного места на диске.
- **GET-NEXT** — расширенный тип запрашивающего сообщения. Может использоваться для просмотра целого дерева объектов управления. Обрабатывая запрос GET-NEXT для конкретного объекта, агент возвращает идентификатор и значение объекта, логически следующего за указанным в запросе, Запрос **GET-NEXT** удобен для динамических таблиц, таких как внутренняя таблица маршрутов IP.
- SET — назначает агенту обновленное значение MIB, если разрешен доступ на запись.
- **GET-BULK** — запрашивает агент узла о передаче максимального объема данных в пределах заданных ограничений по размеру сообщения. Это уменьшает количество пакетов протокола, необходимых для получения большого объема сведений управления. Размер сообщения не должен превышать максимальный блок данных для канала (предельно допустимый размер одного сетевого пакета), иначе может возникнуть фрагментация.
- **NOTIFY** — сообщение, отправляемое агентом SNMP системе управления при обнаружении агентом события определенного типа, возникшего локально на управляемом узле. Консоль управления SNMP, получающую ловушку, называют адресом назначения ловушки. Например, ловушка может быть отправлена в ответ на событие перезагрузки системы.

Вот пример обмена данными между системой управления и агентом (рис. 13-6).

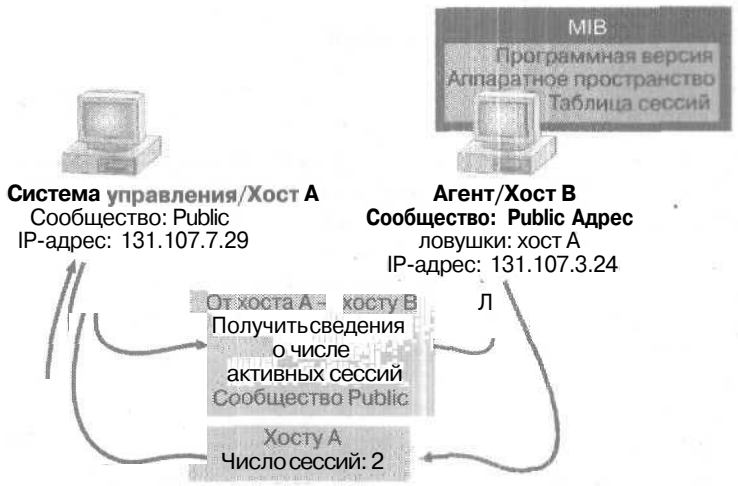


Рис. 13-6. Взаимодействие диспетчера и агента SNMP

Процесс взаимодействия таков:

1. система управления генерирует сообщение SNMP, включающее запрос на получение информации (GET), имя сообщества, к которому относится сама система, и конечный адрес сообщения — IP-адрес агента (131.107.3.24);
2. сообщение SNMP отсылается агенту;
3. агент принимает и расшифровывает пакет, имя сообщества (Public) признается допустимым;
4. для получения из MIB запрошенных сведений о числе сессий служба SNMP вызывает соответствующий субагент;
5. SNMP получает от субагента сведения о числе сессий и генерирует ответное сообщение, включающее информацию о количестве сессий и конечный адрес — IP-адрес системы управления (131.107.7.29);
6. сообщение SNMP отсылается системе управления.

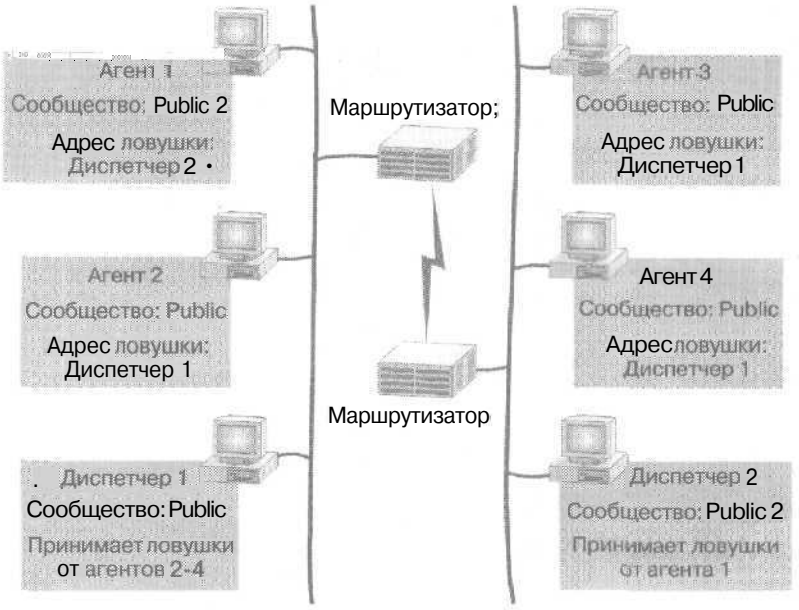
Создание сообществ SNMP

Группы хостов можно объединять в именованные сообщества SNMP для администрирования или обеспечения ограниченной защиты агентов и NMS. Хост может относиться одновременно к нескольким сообществам, однако агент не будет принимать запросы от системы управления, сообщество которой не входит в список допустимых.

Чтобы воспользоваться преимуществами базовой аутентификации, предоставляемой SNMP, сообщества можно организовать логически. На рис. 13-7 показаны сообщества Public и Public 2:

- агент 1 пересылает ловушки и другие сообщения диспетчеру 2, поскольку оба этих хоста относятся к сообществу Public 2;
- агенты 2, 3 и 4 отсылают ловушки и прочие сообщения диспетчеру 1, так как они относятся (по умолчанию) к сообществу Public.

Для задания имен сообществ следует настроить параметры безопасности SNMP. Подробнее о параметрах SNMP см. ниже.



Рис, 13-7. **Пример организации сообществ Public и Public 2**

Примечание Имена сообществ и доменов/рабочих групп никак не связаны. Имена сообществ представляют собой общий пароль, используемый группами сетевых хостов; выбирать и изменять эти имена следует так же, как и пароли. Обычно в сообщества объединяют компьютеры, расположенные недалеко друг от друга.

Установка и настройка службы SNMP

При установке Windows 2000 Server агент SNMP по умолчанию не устанавливается. Для этого служит утилита Add/Remove Programs из Control Panel. В окне этой утилиты щелкните кнопку Add/Remove Windows Components (Добавление и удаление компонентов Windows). Откроется окно мастера Windows Components (Мастер компонентов Windows). Пометьте флажок Management And Monitoring Tools (Средства управления и наблюдения). В состав этой группы компонентов входит Simple Network Management Protocol (Протокол SNMP), по сути являющийся агентом SNMP. После установки данный агент будет отображаться как служба SNMP Service,

А можно настроить службу SNMP из оснастки Computer Management или Services (Службы). Щелкните узел Services и на правой панели выберите SNMP Service. Затем в меню Action (Действие) выберите Properties. Откроется окно свойств службы SNMP (рис. 13-8).

Примечание При установке SNMP устанавливается служба SNMP Trap Service (Служба ловушек SNMP), которая передает ловушки с локального или удаленного компьютера адресату — обычно NMS, выполняющейся на локальном компьютере.

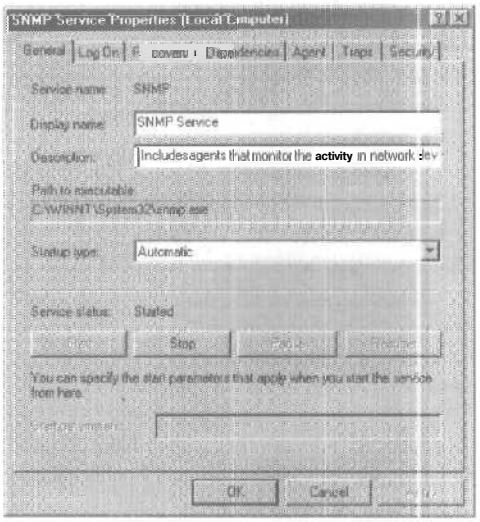


Рис. 13-8. Диалоговое окно свойств службы SNMP

Свойства службы SNMP

Для настройки параметров службы **SNMP,** определяющих порядок запуска, регистрации в системе и восстановления после аварийного завершения работы службы или ОС, используются вкладки General (Общие), Log On (Вход в систему) и Recovery (Восстановление) окна свойств службы. Вкладка General позволяет запустить или остановить службу. **Также** можно указать отображаемое имя, описание, тип и параметры запуска. На вкладке Dependencies (Зависимости) перечислены службы, зависящие от службы **SNMP** (если таковые существуют), и зависимые от нее службы. По умолчанию SNMP зависит от службы Event Log (Журнал событий).

Свойства агента Windows 2000 SNMP

Агент SNMP предоставляет консоли управления информацию об операциях, происходящих на сетевом уровне протокола IP. При получении запроса или ловушки служба SNMP отсылает агенту необходимую информацию.

Для настройки свойств агента служит вкладка Agent (Агент SNMP) окна свойств SNMP, где перечислены доступные службы.

Служба агента	Условия доступности службы
Physical (Физическая)	Компьютер управляет физическими устройствами, например разделом жесткого диска.
Applications (Приложений)	На компьютере установлены приложения, передающие данные по протоколу TCP/IP. Эта служба всегда должна быть включена.
Datalink and subnetwork (Канала данных и подсети)	Компьютер управляет мостом.
Internet (Интернет)	Компьютер является IP-шлюзом (маршрутизатором).
End-to-end (Узел — узел)	Компьютер является узлом (хостом) IP. Эта служба всегда должна быть включена.

Кроме того, на вкладке Agent можно указать имя и координаты человека, например администратора сети, которому в случае сбоя будет послано сообщение. При взаимодействии с агентом SNMP станция управления сетью может запросить эту информацию.

Свойства ловушек

Ловушки SNMP можно использовать для обеспечения ограниченной безопасности. Если для агента настроена служба SNMP, при наступлении определенных событий она будет генерировать сообщения ловушек, которые пересылаются адресату сообщений ловушек; обычно им является станция управления сетью. Например, агент можно настроить так, чтобы при получении запроса на информацию от неизвестной управляющей системы он генерировал ловушку аутентификации. Кроме того, сообщения ловушек можно генерировать для таких событий, как запуск или завершение работы хоста.

Для указания адресов ловушек служит вкладка Traps (Ловушки) окна свойств службы SNMP. Адрес включает имя и IP- или IPX-адрес компьютера, на котором размещается консоль управления. Адресат ловушки должен быть подключенным к сети хостом, на котором выполняется управляющее ПО SNMP. Адреса ловушек могут определяться пользователем, однако события, вызывающие ловушку (например перезагрузка системы), определяет сам агент SNMP.

Параметры безопасности

Для настройки параметров безопасности **SNMP** служит вкладка Security (Безопасность) окна свойств службы SNMP. На ней доступны следующие параметры.

- **Send authentication** traps **(Посылать ловушку проверки подлинности)** — если агент SNMP получит сообщение, не включающее допустимое имя сообщества или отосланное неизвестным хостом, он может отослать одному или нескольким адресатам (консолям управления) сообщение, что запрос SNMP не прошел аутентификацию (по умолчанию).
- Accepted **community names (Приемлемые имена сообществ)** — для службы SNMP следует указать хотя бы одно допустимое имя сообщества. Обычно в качестве имени сообщества используется Public — универсальное для всех реализаций SNMP. Стандартное имя сообщества можно удалить, изменить или добавить новое. Из-за широкой распространенности имя Public небезопасно, поэтому его рекомендуется удалить. При получении запроса из сообщества, отсутствующего в списке допустимых, агент SNMP генерирует ловушку аутентификации. Если имена допустимых сообществ не определены, агент отвергает все входящие запросы SNMP.
- **Community Rights (Права сообщества)** — можно задать уровни разрешений, определяющие порядок обработки агентом SNMP запросов из различных сообществ. Например, Вы можете настроить уровни разрешений так, чтобы агент не обрабатывал запросы из определенного сообщества.
- Accept SNMP packets **from any hosts (Принимать пакеты** SNMP **от любого узла)** — здесь термины «исходный хост» и «список допустимых хостов» означают исходную управляющую систему SNMP и список других допустимых систем управления. Если этот параметр установлен, агент SNMP принимает любые пакеты SNMP, основываясь на имени или адресе исходного хоста и списке допустимых хостов. Данный параметр установлен по умолчанию.
- **Only accept SNMP packets from these hosts (Принимать пакеты SNMP только от этих узлов)** — данный параметр обеспечивает ограниченную безопасность. Если он установлен, агент SNMP принимает пакеты лишь от компьютеров из списка допустимых хостов. Сообщения от других хостов не принимаются, и агент генерирует ловушку аутен-

тификации. Ограничение доступа по списку хостов безопаснее, чем ограничение доступа по списку сообществ, которые могут включать множество компьютеров.

Устранение неполадок SNMP

Далее описываются способы выявления проблем со связью SNMP. Для получения результатов в процессе тестирования создайте реальную нагрузку на систему.

Утилита Event Viewer

В Windows 2000 ручная настройка параметров регистрации ошибок SNMP заменена системой усовершенствованной обработки ошибок, интегрированной с Event Viewer. Если Вам кажется, что служба SNMP сбоит, вызовите Event Viewer.

Служба WINS

Если одни запросы к WINS MIB выполняются, а другие — нет, увеличьте период ожидания SNMP на управляющей системе.

IPX-адреса

Если в процессе установки службы SNMP в качестве имени адреса сообщения ловушки был указан IPX-адрес, при перезагрузке системы Вы можете получить сообщение об ошибке «Error 3». Это происходит, если IPX-адрес указан неверно, т. е. номер сети отделен от MAC-адреса запятой или дефисом. Например, управляющее ПО SNMP воспринимает адреса типа 00008022,0002C0-F7AABD. Тем не менее, служба Windows 2000 SNMP не распознает адреса, в которых номер сети и MAC-адрес разделены запятой или дефисом.

IPX-адрес, указываемый в, адресе сообщения, должен соответствовать формату 8.12, определенному IETF, — xxxxxxxx.yyyyyyyyyyyy, где xxxxxxxx — номер сети, а yyyyyyyyyyyy — MAC-адрес.

Файлы службы SNMP

Эти файлы службы SNMP помогут при решении проблем.

Файл	Описание
Wsnmp32.dll, Mgmtapi.dll	API-интерфейсы диспетчера SNMP перехватывают запросы диспетчера. посылают запросы агентам SNMP и получают от них ответы.
*.dll	DLL-библиотеки агентов-расширений (например, Inet-mib1.dll — библиотека для IIS, а Dhcpmib.dll — для DHCP). Агенты-расширения обеспечивают поддержку собственных форматов MIB соответствующих программных продуктов.
Mib.bin	Устанавливается вместе со службой SNMP и используется API-интерфейсом управления SNMP (Mgmtapi.dll). Содержит привязки текстовых имен объектов к числовым идентификаторам OIDobject.
Snmp.exe	Агентская служба SNMP; мастер-агент (агент-представитель). Принимает запросы диспетчеров и пересылает их для обработки соответствующим DLL-библиотекам субагентов.
Snmptrap.exe	Фоновый процесс. Принимает от агентов SNMP сообщения ловушек и пересылает их интерфейсу управления SNMP в управляющей консоли. Программа запускается лишь после того, как API-интерфейс диспетчера SNMP получит запрос ловушек от диспетчера.

На рис. 13-9 показана совместная работа различных файлов SNMP по обеспечению взаимодействия со станцией управления сетью.

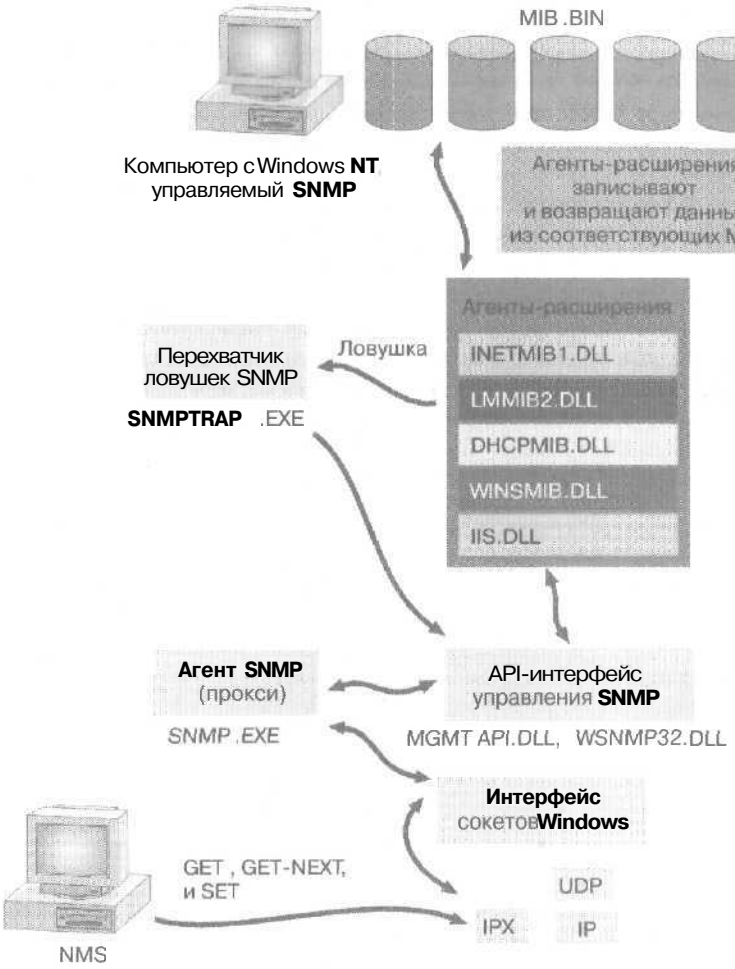


Рис. 13-9. Схема работы службы SNMP

Резюме

SNMP — стандарт управления сетью, позволяющий централизованно контролировать такие сетевые устройства, как серверы, рабочие станции, мосты, маршрутизаторы и концентраторы. Для этого используется распределенная архитектура управляющих систем и агентов. Управляющая система SNMP, обычно называемая станцией управления сетью (NMS), получает информацию от управляемых компьютеров (агентов SNMP) об операциях, происходящих на сетевом уровне протокола IP. Агенты SNMP также отвечают на генерируемые системой управления запросы на получение сведений. В качестве контейнера объектов SNMP использует БД управляющей информации. При этом каждый объект представляет конкретный тип данных. Для контроля и обмена информацией об управляемых объектах агенты и станция управления сетью используют сообщения SNMP. Группы хостов можно объединить в именованные сообщества SNMP для упрощения администрирования или обеспечения ограниченной защиты агентов и систем управления. Для дополнительной защиты можно указать IP-адрес или хост-имя системы управления сетью, с которой должен взаимодействовать агент SNMP. Для настройки службы SNMP воспользуйтесь узлом Services (Службы) оснастки Computer Management (Управление компьютером) или оснасткой Services (Службы) в меню Start\Programs\Administrative Tools (Пуск\-Программы\Администрирование). Параметры SNMP настраиваются в окне свойств службы SNMP.

Занятие 13 Консоль Performance

В Windows 2000 предусмотрены две утилиты для мониторинга использования ресурсов компьютера — оснастки System Monitor (Системный монитор) и Performance Logs And Alerts (Оповещения и журналы производительности), предустановленные в консоль Performance (Производительность). System Monitor позволяет отслеживать использование ресурсов и пропускную способность сети. С помощью Performance Logs And Alerts можно собирать сведения о производительности локальных и удаленных компьютеров.

Изучив материал этого занятия, Вы сможете:

- ✓ использовать оснастки System Monitor и Performance Logs And Alerts консоли Performance для мониторинга ресурсов компьютера.

Продолжительность занятия — около 40 минут.

Основы работы с консолью Performance

Консоль Performance (Производительность) — встроенная утилита меню Start\Programs\Administrative Tools, представляющая собой консоль MMC, включающую предустановленные оснастки System Monitor и Performance Logs And Alerts (рис. 13-10).

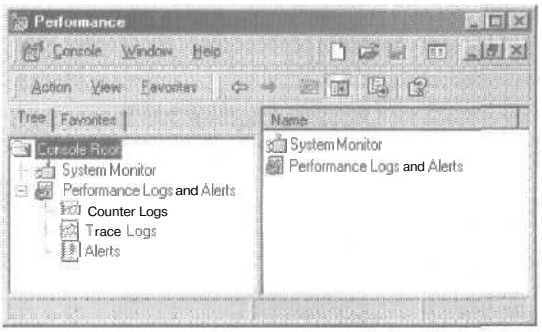


Рис. 13-10. Оснастки System Monitor (Системный монитор) и Performance Logs And Alerts (Оповещения и журналы производительности)

При помощи System Monitor можно в реальном времени собирать данные о памяти, дисках, процессоре, сети и прочих операциях и просматривать полученную информацию в форме графиков, гистограмм или отчетов. Performance Logs And Alerts позволяет сконфигурировать журналы для регистрации данных о производительности. Также можно настроить сигналы оповещения уровня системы, извещающие о том, что значение определенного счетчика превысило или опустилось ниже заданного порога.

Мониторинг производительности системы является важной составной частью поддержки и администрирования Windows 2000 Server. Полученные сведения можно использовать для:

- определения реальной рабочей нагрузки и ее влияния на ресурсы системы;
- анализа изменений и тенденций в рабочей нагрузке и в использовании ресурсов, который поможет спланировать будущую модернизацию системы;
- мониторинга результатов настройки системы или результатов изменений в конфигурации;
- выявления проблем и компонентов или процессов, требующих оптимизации.

Оснастки System Monitor и Performance Logs And Alerts предоставляют подробные сведения о ресурсах, используемых конкретными компонентами ОС и программами сервера, разработанными для сбора данных о производительности. Графики отображают данные, собранные в ходе мониторинга производительности. Журналы позволяют сохранить эти данные. Сигналы оповещения при помощи службы Messenger (Служба сообщений) рассылают пользователям сообщения в случае, если значение счетчика достигнет, превысит или упадет ниже заданного порога.

Данные мониторинга производительности используют специалисты службы технической поддержки. Поэтому мониторинг надо выполнять регулярно.

Оснастка System Monitor

Оснастка System Monitor (Системный монитор), заменившая в Windows 2000 утилиту Performance Monitor, позволяет осуществлять мониторинг производительности системы и других компьютеров сети. System Monitor служит для:

- сбора в реальном времени и просмотра данных о производительности локального и удаленных компьютеров;
- просмотра текущих или старых данных, хранящихся в журнале счетчика;
- просмотра данных в виде графика, гистограммы или отчета;
- включения функциональности System Monitor в Microsoft Word и других приложений пакета Microsoft Office при помоши *Автоматизации* (Automation);
- создания HTML-страниц из представлений данных о производительности;
- создания конфигураций для мониторинга, которые можно установить на другие компьютеры, использующие MMC.

System Monitor позволяет собирать и просматривать данные об использовании аппаратных ресурсов компьютеров и об активности системных служб. Для этого служат следующие параметры.

- **Тип** данных. Чтобы ограничить диапазон регистрируемых данных, укажите один или несколько экземпляров счетчиков или объектов мониторинга производительности. У некоторых объектов (например, Memory) предусмотрены счетчики, предоставляющие данные о системных ресурсах. У других — счетчики, предоставляющие информацию о работе приложений (например о работе системных служб или приложений Microsoft BackOffice).
- Источник данных. System Monitor может собирать сведения о локальном компьютере или о других компьютерах в сети, к которым у Вас есть доступ (по умолчанию нужны права администратора). Кроме того, можно включить любые данные, собираемые в реальном времени, или данные журналов.
- Способ **выборки.** System Monitor поддерживает ручную выборку, автоматическую выборку с заданным интервалом и выборку по запросу. При просмотре журнала для отбора данных можно указать временной интервал.

Интерфейс оснастки System Monitor

При запуске консоли Performance (Производительность) по умолчанию отображается график и панель инструментов. Сначала график пуст. После добавления счетчиков в области графика появятся кривые значений счетчиков (рис. 13-11; на рисунке не показано дерево консоли).

График

Данные System Monitor могут обновляться автоматически или по запросу. Чтобы начать обновление данных по запросу, щелкните кнопку Update Data (Обновить данные) (кнопка со значком фотоаппарата на панели инструментов), затем щелкните ее еще раз, чтобы остановить процесс сбора информации. Для очистки графика щелкните кнопку Clear Display (Очистить экран) (вторая слева кнопка на панели инструментов). Чтобы добавить счетчики, щелкните кнопку Add (Добавить) (кнопка со значком «+» на панели инструментов) и в диалоговом окне Add Counters (Добавить счетчики) выберите счетчики.

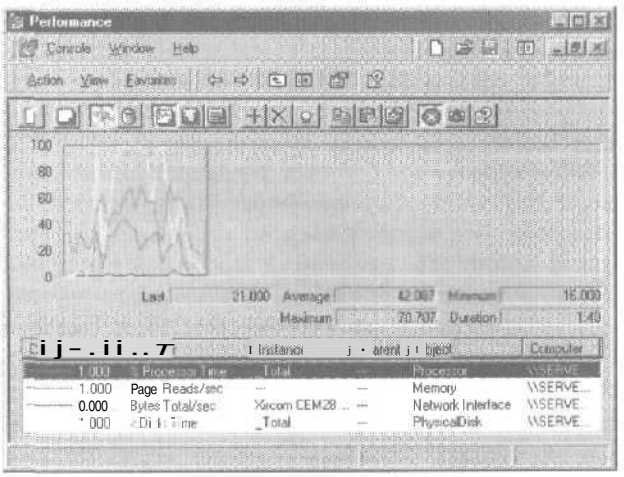


Рис. 13-11. Отображение изменений значений счетчиков в оснастке System Monitor

Как видите, интерфейс System Monitor включает три основных элемента: график, его легенду и панель значений.

Перемещение линии таймера (вертикальная линия на рис. 13-11) вдоль графика соответствует прошествию очередного интервала обновления. Независимо от величины интервала обновления представление отображает до 100 выборок. По мере необходимости System Monitor сжимает данные журнала, чтобы вместить построенный на их основе график в пределы экрана. Для просмотра сжатых данных журнала щелкните кнопку Properties (Свойства) (четвертая кнопка справа на панели инструментов), перейдите на вкладку Source (Источник), выберите файл журнала и укажите более короткий интервал времени, который включает меньше данных, и вероятность того, что частные значения не будут отображены, снижается.

Также можно конфигурировать следующие параметры графика:

- тип отображения с отдельными настройками для графиков, гистограмм и отчетов;
- цвет фона панели деталей и области отображения данных;
- размер, тип и стиль шрифта, используемого для отображения текста;
- цвет, ширину и стиль линий диаграмм.

Для привлечения внимания к данным конкретного счетчика служит функция выделения. Нажмите Ctrl+H или щелкните кнопку Highlight (Выделить) (кнопка со значком лампочки) на панели деталей. При использовании выделения цвет столбца или линии, отображающей данные выбранного счетчика, изменяется на белый (для темных цветов фона, включая цвет фона по умолчанию) или черный (для светлых цветов фона).

Примечание Клавиатурные сокращения Microsoft Word могут конфликтовать с сокращением Ctrl+H, используемым в System Monitor для выделения данных счетчика. Если элемент управления System Monitor (%systemroot%System32\Sysmon.ocx) будет использоваться в Microsoft Word, измените комбинации клавиш последнего.

Легенда

Легенда (набор обозначений и пояснений к ним под графиком) отображает сведения о выбранных счетчиках и включает такие поля.

- **Object (Объект).** Представляет собой логический набор счетчиков, связанный с ресурсом или службой, доступной для мониторинга.
- **Counter (Счетчик).** Это элемент данных, связанный с объектом. Для каждого выбранного счетчика System Monitor отображает значение, соответствующее некоторому аспекту производительности, определенному для объекта.
- **Instance (Экземпляр).** Термин *экземпляр объекта* используется для различения нескольких экземпляров одного счетчика. По умолчанию перечисленные экземпляры счетчика отсортированы по имени и числовому индексу, указываемому после имени экземпляра (знак # и число). Он упрощает мониторинг нескольких экземпляров счетчика, например, при наблюдении за потоками процесса. Чтобы отключить отображение индекса, щелкните кнопку Properties (Свойства) и снимите флажок Allow Duplicate Counter Instances (Допускать дублирование счетчиков).

Сортировка элементов может осуществляться по возрастанию/убыванию, по объекту, счетчику, экземпляру или компьютеру. Для этого достаточно щелкнуть соответствующий столбец легенды. Например, чтобы отсортировать все записи по имени, щелкните столбец Counter (Счетчик).

Примечание Чтобы выделить в легенде счетчик, соответствующий одной из линий, дважды щелкните любую точку этой линии. Если линии графика расположены слишком близко, найдите место, где они расходятся. В противном случае System Monitor может неверно выделить счетчик.

Панель значений

Панель значений находится между областью графика и легендой; она содержит последнее (Last), среднее (Average), минимальное (Minimum) и максимальное (Maximum) значения выбранного счетчика. Значения вычисляются по периоду времени и числу выборок, отображаемому в области графика, а не по периоду времени с начала мониторинга. Значение Duration (Длительность) в панели значений показывает общее время, отражаемое графиком (зависит от интервала обновления).

Мониторинг производительности сети и системы

Сетевая активность может влиять не только на производительность сетевых компонентов Вашей системы, но и на производительность системы в целом. Наряду с мониторингом уровня сетевой активности следует также вести мониторинг других компонентов, например дисков, памяти и активности процессора. System Monitor позволяет осуществлять мониторинг активности сети и системы при помощи одной утилиты.

Для обычного мониторинга используют следующие счетчики:

- Cache\Data Map Hits % (Кэш\% попаданий при отображении данных);
- Cache\Fast Reads/sec (Кэш\Быстрых чтений/сек);
- Cache\Lazy Write Pages/sec (Страниц «ленивой» записи/сек);

- Logical Disk\% Disk Space (Файл подкачки\% использования);
- Memory\Available Bytes (Память\Доступно байт);
- Memory\Nonpaged Pool Allocs (Память\Распределений в невыгружаемом страничном пуле);
- Memory\Nonpaged Pool Bytes (Память\Байт в невыгружаемом страничном пуле);
- Memory\Paged Pool Allocs (Память\Распределений в выгружаемом страничном пуле);
- Memory\Paged Pool Bytes (Память\Байт в выгружаемом страничном пуле);
- Processor (Total)\Interrupts/sec (Процессор\Прерываний/сек);
- Processor (Total)\% Processor Time (Процессор\% загруженности процессора);
- System\Context Switches/sec (Система\Контекстных переключений/сек);
- System\Processor Queue Length (Система\Длина очереди процессора).

Мониторинг сетевой активности при помощи System Monitor включает изучение сведений о производительности каждого уровня модели OSI. System Monitor предоставляет объекты производительности для сбора данных о скорости передачи, длине очереди пакетов и прочей информации о быстродействии сети.

Примечание В связи с нагрузкой, создаваемой заголовками протокола, реальная скорость передачи может отличаться от скорости, указанной для используемого провода или канала.

Ниже перечислены уровни модели OSI и объекты производительности, используемые для наблюдения за этими уровнями.

Уровень модели OSI	Объекты производительности
Прикладной, представительский, сеансовый	Browser (Обозреватель сети), Server (Сервер), Redirector (Перенаправитель) и Server Work Queues NBT Connection (Рабочие очереди сервера). NBT — сокращение от NetBIOS over TCP/IP.
Транспортный	Объекты протокола: TCP для Transmission Control Protocol, UDP для User Datagram Protocol, NetBEUI для NetBIOS, AppleTalk (устанавливается протоколом).
Сетевой	Network Segment (устанавливается вместе с драйвером Network Monitor), IP для Internet Protocol, NWLink IPX/SPX для реализации стека протоколов IPX/SPX производства Microsoft. Счетчики объектов производительности NWLink, отображающие активность кадров, будут показывать нули. При установке агента Network Monitor Agent на системах с Windows NT 4.0 также устанавливаются счетчики Network Segment.
Канальный, физический	Network Interface (Сетевой интерфейс). Эти счетчики поддерживаются драйвером и из-за проблем, связанных с реализацией счетчиков драйвером, могут отображать неверные или нулевые значения.

При мониторинге данных о производительности сети следует переходить от компонентов нижнего уровня к более высоким уровням. Ведите наблюдение за объектами в течение периода, продолжительность которого может составлять от нескольких дней до нескольких месяцев. Используя полученные данные, определите *эталонный уровень производительности* — уровень производительности системы при типичной рабочей нагрузке, который позволит Вам сравнивать производительность в разные периоды времени и выявлять тенденции, потребности и узкие места. Если производительность в пределах эталонного уровня становится неудовлетворительной, настройте сеть.

Как и для прочих ресурсов, задайте параметры эталонного уровня производительности сети. При падении производительности ниже допустимого уровня, выясните его причину. Ненормальные значения сетевых счетчиков зачастую указывают на проблемы с памятью, процессором или дисками сервера. Поэтому при мониторинге сервера в дополнение к счетчикам сети также рекомендуется использовать счетчики Processor\% Processor Time (Процессор\% загруженности процессора), PhysicalDisk\% Disk Time (Физический диск\% активности диска) и Memory\Pages/sec (Память\Обмен страниц/сек).

Например, если рост значений счетчика Pages/sec сопровождается ростом значений счетчика Bytes Total/sec, серверу, вероятно, не хватает физической памяти для сетевых операций. Многие сетевые ресурсы, включая сетевые адаптеры и ПО протоколов, используют физическую память. Высокий уровень подкачки страниц может быть вызван тем, что почти вся физическая память выделена сетевым операциям, и для процессов, использующих виртуальную память, оставлен лишь небольшой объем ПЗУ. Чтобы убедиться в этом, проверьте в журнале событий наличие записей о том, что закончилась физическая или виртуальная память. Кроме того, осуществляйте мониторинг физической памяти пула и прочих счетчиков памяти.

Объекты диска и утилита Diskperf

Объекты диска PhysicalDisk и LogicalDisk содержат счетчики в System Monitor. По умолчанию в Windows 2000 Server включены счетчики производительности физических дисков и отключены счетчики производительности логических. Для их включения запустите утилиту командной строки Diskperf с параметром yv (diskperf – yv).

После этого перезагрузите компьютер — запустятсяя счетчики производительности логических и физических дисков, которые содержатся в объектах LogicalDisk и PhysicalDisk оснастки System Monitor.

Работа этих счетчиков несколько снижает производительность системы. Если Вы не ведете мониторинг производительности дисков, отключите объекты диска и их счетчики командой diskperf –n.

Diskperf позволяет выборочно включать и отключать счетчики производительности логических и физических дисков.

Оснастка Performance Logs And Alerts

Оснастка Performance Logs and Alerts (Оповещения и журналы производительности) позволяет автоматически собирать данные о производительности локальных и удаленных компьютеров. Для просмотра собранных сведений можно использовать System Monitor или экспортировать данные в программы для работы с электронными таблицами или БД для анализа и создания отчетов. Поскольку ведение журнала осуществляется в виде службы, сбор данных может происходить независимо от того, работает ли кто-нибудь на наблюдаемом компьютере.

Performance Logs And Alerts позволяет:

- собирать данные в текстовые файлы, разделенные запятыми или знаками табуляции для импорта в программы для работы с электронными таблицами; для цикличного сбора информации и для сбора сведений о таких элементах, как потоки и процессы, которые могут стартовать после начала сбора информации, используется двоичный формат файла журнала (цикличный сбор информации — непрерывная запись данных в один файл с заменой старых данных новыми);
- просматривать данные счетчика в процессе их сбора или после его завершения;
- определять время начала и останова, имена и размеры файлов, а также другие параметры автоматического создания файлов журнала;

- управлять несколькими сеансами из одного окна консоли;
- определять для счетчика сигнал оповещения, чтобы в случае превышения значения счетчика или падения его ниже заданного предела отсылалось сообщение, запускалась программа или начиналось ведение журнала.

Как и System Monitor, оснастка Performance Monitor поддерживает:

- выбор объектов и счетчиков производительности и экземпляров объектов;
- задание интервалов выборки для мониторинга аппаратных ресурсов и системных служб.

Performance Logs And Alerts предоставляет следующие возможности по регистрации данных о производительности.

- Запуск и останов ведения журнала — ручной или автоматический по определенному пользователем расписанию.
- Создание трассировочных отчетов. Используя системного поставщика данных по умолчанию или какого-либо другого поставщика, трассировочные отчеты фиксируют данные при выполнении системой определенных действий, например при операциях дискового ввода/вывода или при ошибках памяти. При наступлении события поставщик посылает данные службе Performance Logs And Alerts. Такая запись и пересылка данных отличается от работы счетчиков журналов, при которой служба получает данные от системы по истечении интервала обновления, а не при наступлении определенного события. При работе с выводом трассировочного журнала создается синтаксический анализатор. Создать его позволяют API-интерфейсы, доступные по адресу http://msdn.microsoft.com/.
- Выбор программы, запускаемой после останова ведения журнала.
- Настройка дополнительных параметров автоматического ведения журнала, включая автоматическое переименование файлов и задание времени запуска/останова журнала, основанных на прошедшем интервале времени или размере файла.

Примечание С данными файла журнала можно работать, пока служба собирает информацию и файл заблокирован. Например, Microsoft Excel может импортировать активный файл журнала, однако файл будет доступен лишь для чтения.

Интерфейс оснастки Performance Logs And Alerts

В оснастке Performance Logs And Alerts можно определить параметры журналов счетчиков, трассировочных счетчиков и сигналов оповещения, Созданные Вами журналы и сигналы оповещения отображаются в правой панели (рис. 13-12).

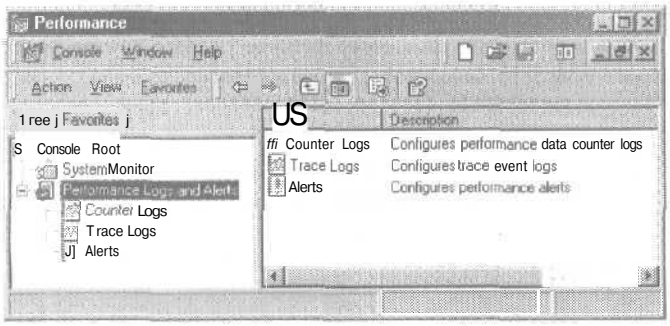


Рис. 13-12. Журналы и сигналы оповещения, отображаемые в правой панели оснастки Performance Logs And Alerts

Оснастку можно настроить для одновременного ведения нескольких журналов или одновременного срабатывания нескольких сигналов оповещения. Все журналы и сигналы оповещения сохраняются с определяемой Вами конфигурацией. Журнал, настроенный для автоматического запуска и останова, может создать несколько отдельных файлов журнала. Например, если журнал регистрирует сведения об активности системы за день, то один файл будет закрыт в 23:59 текущего дня, а другой — открыт в 00:00 следующего.

Ниже описаны поля правой панели.

Поле	Описание
Name (Название)	Имя журнала или сигнала оповещения. Можно считать его «понятным именем», описывающим наблюдаемое условие или тип собираемых данных. Журнал может создавать несколько файлов. Для регистрации показаний счетчиков был создан образец файла журнала с именем System Overview. Вы можете воспользоваться этим файлом или определить свои параметры регистрации данных.
Comment (Комментарий)	Описание журнала или сигнала оповещения.
Log File Type (Тип журнала)	Определяемый Вами формат файла журнала. Тип сигналов оповещения указывается как «alerts», а тип трассировочных журналов — как «sequential». Типы журналов: binary (двоичный), binary circular (двоичный циклический), text-CSV (текстовый файл — CSV для текста, разделенного запятыми) или text-TSV (текстовый файл — TSV для текста, разделенного символами табуляции).
Log File Name (Имя файла журнала)	Путь и основное имя файла журнала. Может автоматически дополняться суффиксом, указывающим на дату сбора информации.

Чтобы просмотреть параметры журнала, отметьте его в панели деталей и выберите команду Properties (Свойства) в меню Action (Действие). В открывшемся диалоговом окне можно определить параметры именования файлов журнала, время регистрации данных, используемые счетчики и объекты производительности.

Если журнал в данный момент собирает данные, рядом с именем журнала или сигнала оповещения отображается зеленый значок данных. Красный значок указывает, что параметры файла журнала или сигнала оповещения определены, но файл или журнал в данный момент неактивны.

Примечание Performance Monitor можно настроить для одновременного ведения журналов нескольких типов. Если выбран параметр перезапуска или если Вы многократно останавливаете и запускаете журнал, он может создать несколько файлов. Однако они не будут отображаться в окне консоли. Просмотреть их позволяет Windows Explorer.

Резюме

Консоль Performance из меню Start\Programs\Administrative Tools содержит две утилиты для мониторинга использования ресурсов компьютера — оснастки System Monitor и Performance Logs And Alerts. System Monitor позволяет определять производительность локального и удаленных компьютеров. При помощи System Monitor можно собирать подробные сведения об использовании аппаратных ресурсов и активности системных служб компьютеров. Интерфейс System Monitor включает три основных элемента: область графика, легенду и панель значений- В System Monitor имеются объекты производительности для сбора данных о скорости передачи, очереди пакетов и прочей информации о быстродействии сети. Каждый объект представляет собой логический набор счетчиков. Для каждого выбранного счетчика отображается значение, соответствующее некоторому аспекту производительности, определенному для объекта. Performance Logs And Alerts позволяет автоматически собирать сведения о производительности локальных и удаленных компьютеров. Как и System Monitor, Performance Logs And Alerts позволяет выбирать используемые объекты, счетчики производительности и экземпляры объектов, а также задавать интервалы выборки для мониторинга аппаратных ресурсов и системных служб. В оснастке Performance Logs And Alerts можно определить параметры журналов счетчиков, трассировочных счетчиков и сигналов оповещения. Созданные Вами журналы и сигналы оповещения отображаются на правой панели консоли.

Занятие 1. Утилита Network Monitor

Утилита Network Monitor (Сетевой монитор) служит для просмотра сетевой активности и выявления проблем сети. Например, если два компьютера не могут установить между собой связь, Network Monitor поможет выявить программные и аппаратные проблемы. Кроме того, можно скопировать журнал сетевой активности в файл и переслать его профессиональному аналитику сети или службе поддержки. Разработчики сетевых приложений используют Network Monitor для мониторинга и отладки создаваемых сетевых программ.

Изучив материал этого занятия, Вы сможете:

- ✓ использовать Network Monitor для перехвата и отображения сетевых кадров.

Продолжительность занятия - около 35 минут.

Возможности Network Monitor

Network Monitor отслеживает пропускную способность сети, записывая сетевой трафик. Утилита осуществляет мониторинг лишь трафика локального сегмента сети. Для мониторинга удаленного трафика следует использовать версию Network Monitor, поставляемую с Microsoft Systems Management Server (SMS) версии 1.2 или 2.0.

Network Monitor отслеживает поток сетевых данных, передаваемых по сети в настоящее время. Перед передачей сетевое ПО делит информацию на небольшие блоки — кадры, или пакеты. Каждый пакет включает:

- адрес компьютера, пославшего сообщение;
- адрес компьютера, который должен получить кадр;
- заголовки протоколов, используемых для передачи кадра;
- данные или часть пересылаемой информации;
- циклическую контрольную сумму для контроля целостности кадра.

Процесс копирования пакетов называется *перехватом*. Network Monitor позволяет записать весь сетевой трафик или отдельный набор пакетов. Перехват можно настроить и для реагирования на события сети. Например, можно сделать так, чтобы сеть запускала исполнимый файл, если Network Monitor обнаружит определенные условия. Это аналогично системной команде Alerts, доступной в оснастке Performance Logs And Alerts.

Network Monitor позволяет просмотреть записанные данные. Эта утилита выполняет большую часть работы по анализу данных, преобразуя записанные данные в логическую структуру пакетов.

В целях безопасности Windows 2000 Network Monitor перехватывает лишь входящие/исходящие пакеты локального компьютера, включая пакеты групповых и широковещательных рассылок. Помимо этого, Network Monitor отображает общую статистику по сегменту сети для пакетов широковещательных и многоадресных рассылок, степень загруженности сети и количество принятых и переданных за секунду байт.

Для защиты сети от несанкционированно установленных утилит Network Monitor эта утилита может распознавать другие свои экземпляры, выполняющиеся в локальном сегменте сети. Network Monitor также распознает все экземпляры драйвера Network Monitor (утилиты Network Monitor из Systems Management Server или объекта Network Segment из System Monitor), используемого для удаленного перехвата данных Вашей сети.

При обнаружении других экземпляров Network Monitor, выполняющихся в сети, утилита выводит:

- имя компьютера, на котором установлен выполняющийся экземпляр;
- имя пользователя, зарегистрированного в данный момент на этом компьютере;
- состояние Network Monitor на удаленном компьютере (выполняется, захватывает или передает данные);
- адрес сетевой платы на удаленном компьютере;
- номер версии Network Monitor на удаленном компьютере.

Иногда архитектура сети не позволяет Network Monitor обнаруживать другие экземпляры утилиты в сети. Например, если установленный экземпляр Network Monitor отделен от Вашего маршрутизатором, не транслирующим многоадресные пакеты, Вы не обнаружите удаленный экземпляр утилиты.

Для копирования всех перехватываемых пакетов в буфер (область хранения с изменяемым размером в памяти) используется одна из функций интерфейса **NDIS.** Размер буфера по умолчанию — 1 Мб, но его можно изменить. Буфер является файлом с привязкой к памяти и занимает дисковое пространство.

Примечание Поскольку Network Monitor использует локальный, а не смешанный режим NDIS (в котором сетевая плата ретранслирует все пакеты, пересылаемые в сети), с этой утилитой можно работать, даже если Ваша сетевая плата не поддерживает смешанный режим. (При ее переводе в смешанный режим прирост нагрузки на процессор может составить до 30%.)

Установка средств Network Monitor

Средства Network Monitor включают консоль Network Monitor и драйвер Network Monitor. По умолчанию данные утилиты не устанавливаются вместе с Windows 2000 Server. Для их установки служит приложение Add/Remove Programs из Control Panel. В левой панели утилиты щелкните кнопку Add/Remove Windows Components. Откроется окно мастера Windows Components (Мастер компонентов Windows). Пометьте в списке компонентов флажок Management And Monitoring Tools (Средства управления и наблюдения) и щелкните кнопку Details (Состав). В открывшемся окне пометьте флажок Network Monitor Tools (Средства сетевого монитора) и дважды щелкните кнопку OK. После установки консоль Network Monitor (Сетевой монитор) появится в меню Start\Programs\Administrative Tools, а драйвер — в диалоговом окне свойств подключения к локальной сети.

Перехват пакетов

Для перехвата пакетов на компьютере с Windows 2000 должны быть установлены утилита и драйвер Network Monitor. Драйвер Network Monitor (также называемый агентом Network Monitor) позволяет стандартной утилите Network Monitor получать кадры от сетевой платы, а утилите Network Monitor, поставляемой в составе SMS, — перехватывать и выводить информацию пакетов с удаленных компьютеров. Когда компьютер с SMS Network Monitor удаленно подключается к компьютеру с драйвером Network Monitor и начинает запись кадров, он осуществляется локально, на компьютере с драйвером Network Monitor, а вывод данных — на управляющем компьютере с SMS Network Monitor.

Примечание Вместе с SMS поставляются драйверы Network Monitor для других ОС семейства Windows. При установке Network Monitor на компьютере Windows 2000 автоматически устанавливается драйвер Network Monitor.

Для записи данных запустите Network Monitor и в меню Capture (Запись) выберите команду Start (Запустить). По мере захвата кадров в окне Network Monitor будет отображаться статистическая информация (рис. 13-13).

Network Monitor отображает статистику для первой сотни обнаруженных уникальных сессий. Чтобы просмотреть сведения о следующей сотне сессий, в меню Capture выберите команду Clear Statistics (Очистить статистику).

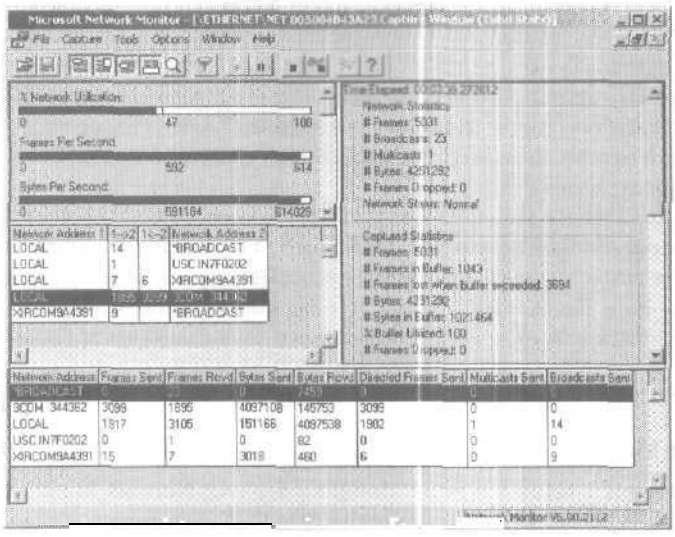


Рис. 13-13. Утилита Network Monitor со статистической информацией

Использование фильтров

Фильтр записи аналогичен запросу к БД и применяется для отбора наблюдаемых сведений о сети. Так, для наблюдения за определенным поднабором компьютеров или протоколов можно создать БД адресов, добавить в нее отбираемые адреса и сохранить фильтр в файл. Фильтрация пакетов позволяет сэкономить время и ресурсы буфера. При необходимости Вы можете воспользоваться файлом фильтра.

Чтобы определить фильтр записи, укажите в диалоговом окне Capture Filter (Фильтр записи) (рис.13-14) условные операторы.

В меню Capture (Запись) выберите команду Filter (Фильтр), щелкните на панели инструментов кнопку со значком воронки (рис. 13-14) или нажмите клавишу FS. В диалоговом окне Capture Filter отображается дерево условий фильтра, графически представляющее его логику. Добавление или исключение информации из параметров записи отображается в дереве условий.

Фильтрация по протоколу

Для отбора кадров, использующих определенный протокол, укажите его в строке SAP/ETYPE= фильтра. Например, для записи только IP-кадров отключите все протоколы и затем включите IPETYPE 0x800 и IP SAP 0x6. По умолчанию включены все протоколы, поддерживаемые Network Monitor.

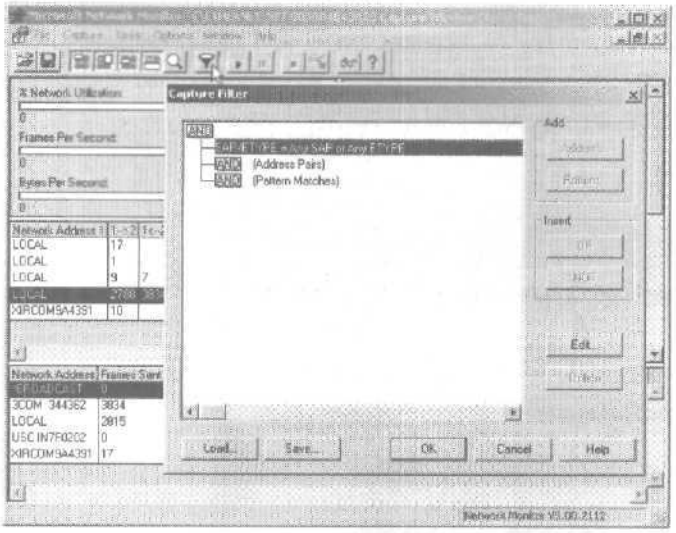


Рис. 13-14. Диалоговое окно Capture Filter (Фильтр записи)

Фильтрация по адресу

Для отбора пакетов, поступающих с компьютеров сети, укажите в фильтре одну или несколько пар адресов. Можно одновременно осуществлять мониторинг до 4 пар адресов, включающих:

- адреса компьютеров, трафик между которыми требуется наблюдать;
- стрелки, указывающие направление наблюдаемого трафика;
- ключевое слово INCLUDE или EXCLUDE, определяющее, как Network Monitor должен реагировать на кадр, соответствующий условию фильтра.

Независимо от последовательности отображения операторов в диалоговом окне Capture Filter, первыми выполняются операторы EXCLUDE. Следовательно, если кадр соответствует параметрам оператора EXCULDE, а фильтр содержит как оператор EXCLUDE, так и оператор INCLUDE, кадр отбрасывается, и Network Monitor не проверяет его на соответствие параметрам оператора INCLUDE.

Фильтрация по шаблону

Шаблон соответствия, указанный в фильтре захвата, позволяет:

- ограничить перехват кадрами, содержащими заданную комбинацию **ASCII-** илишестнадцатеричных данных;
- указать смещение шаблона в кадре.

При фильтрации данных по шаблону надо указать смещение шаблона в кадре (через сколько байт от начала или конца файла должна размещаться комбинация, соответствующая шаблону). Если в среде передачи используются кадры переменной длины, укажите, что смешение должно отсчитываться от конца заголовка топологии.

Вывод записанных данных

Network Monitor преобразует собранные чистые данные и отображает их в окне Capture. Чтобы в процессе записи отобразить в окне Capture полученные данные, выберите в меню Capture (Запись) команду Stop And View (Остановить и просмотреть) или откройте файл с расширением .cap. Если Вы остановили процесс записи, для просмотра данных можно

выбрать команду Display Captured Data (Отобразить записанные данные) в меню Capture, щелкнуть на панели инструментов кнопку со значком очков или нажать клавишу F12 (рис. 13-15).

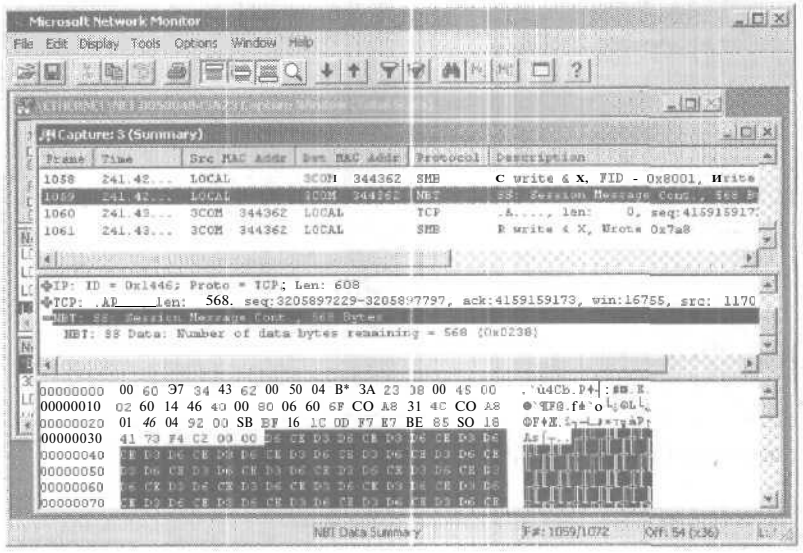


Рис. 13-15. Окно Capture утилиты Network Monitor

Использование фильтров отображения

Как и фильтр записи, фильтр отображения аналогичен запросу к БД и позволяет отобрать нужную информацию. Однако поскольку фильтр вывода работает с уже записанными данными, он не влияет на содержимое буфера захвата Network Monitor.

Отображаемые кадры можно фильтровать по:

- исходному или конечному адресу;
- протоколам, использованным для пересылки кадра;
- свойствам и значениям, содержащимся в кадре (свойство — это поле данных заголовка протокола; свойства протокола указывают его назначение).

Чтобы открыть окно Display Filter (Фильтр записи) (рис. 13-16), перейдите в окно Network Monitor, воспользуйтесь меню Display (Сервис), нажмите клавишу F8 или щелкните на панели инструментов кнопку со значком воронки.

Чтобы определить фильтр отображения, укажите в окне Display Filter условные операторы. В этом окне отображается дерево условий фильтра, графически представляющее его логику. В дереве отображается добавление или исключение информации из параметров вывода. Прежде чем добавить следующий оператор, щелкните OK, чтобы сохранить выбранный оператор и добавить его в дерево условий.

Фильтры отображения, в отличие от фильтров записи, не ограничены 4 адресами. Кроме того, они позволяют использовать логические операторы AND, OR и NOT. При отображении записанных данных в окне Frame Viewer выводится вся имеющаяся о них информация. Для отображения кадров, переданных с использованием конкретного протокола, отредактируйте в диалоговом окне Display Filter строку Protocol.

Свойства протокола определяют его назначение. Допустим, Вы записали много кадров, использующих протокол SMB, и Вам требуется изучить лишь те, в которых этот про-

токол использовался для создания на Вашем компьютере каталога. В этом случае можно выбрать кадры, в которых свойство SM B Command соответствует команде Make Directory.

При выводе записанных данных в окне Frame Viewer отображаются все адреса, с которых была захвачена информация. Для отображения кадров, полученных с определенного компьютера, отредактируйте в диалоговом окне Display Filter строку ANY< – >ANY.

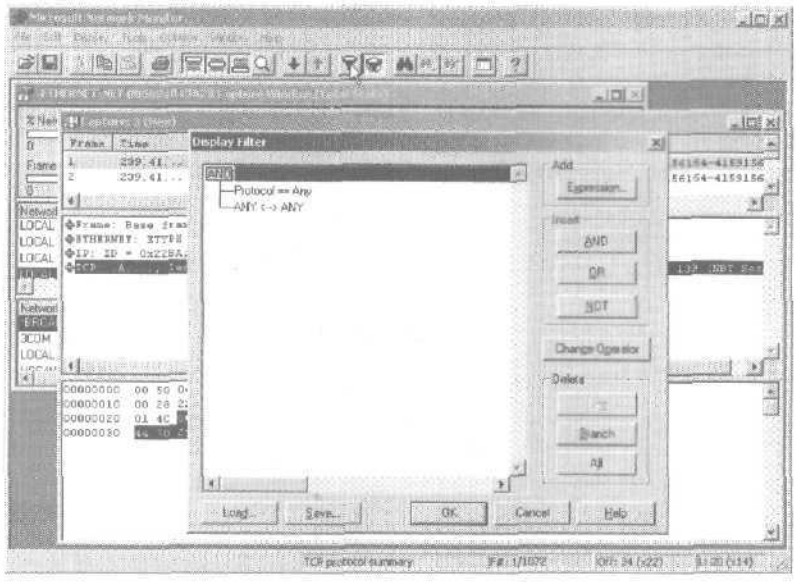


***Рис.* 13-16. Диалоговое окно Display Filter**

Оптимизация производительности Network Monitor

Network Monitor создает для буфера записи привязанный к памяти файл. Для оптимальной производительности убедитесь, что размер созданного Вами буфера соответствует текущему трафику.

Кроме тото, хотя Вы и не можете изменять размер кадра, можно сохранять лишь часть кадра, тем самым уменьшая объем используемого пространства буфера. Например, если Вас интересуют лишь данные заголовка кадра, установите размер кадра (в байтах) равным размеру заголовка. При записи кадров в буфер Network Monitor сохранит лишь заголовок.

Чтобы уменьшить объем системных ресурсов, необходимый для работы Network Monitor, запускайте утилиту в фоновом режиме. В меню Capture (Запись) выберите команду Dedicated Mode Capture (Режим выделенной записи). Это единственный способ снизить требования к объему необходимых ресурсов в случае, если сетевые пакеты теряются, а не перехватываются.

Резюме

Утилита Network Monitor позволяет просматривать и выявлять проблемы сети. Она отслеживает пропускную способность сети, записывая сетевой трафик. Network Monitor осуществляет мониторинг потока сетевых данных, состоящего из всей информации, передаваемой по сети в текущий момент. Для записи кадров на компьютере с Windows 2000 нужно установить утилиту и драйвер Network Monitor, который позволяет Network Monitor получать кадры от сетевой платы. Фильтр записи аналогичен запросу к БД. Фильтры можно применять для отбора наблюдаемых сведений о сети, Network Monitor преобразует чистые перехваченные данные и выводит их в окне Frame Viewer. Фильтры отображения позволяют выбирать сведения, отображаемые в окне Frame Viewer. Как и фильтр записи, фильтр отображения аналогичен запросу к БД и позволяет отобрать нужную информацию.

Занятие 5. Утилита Task Manager

Утилита Windows Task Manager (Диспетчер задач) предоставляет суммарную информацию о производительности компьютера, о программах и процессах, выполняющихся в системе, Она позволяет завершать работу программ и процессов, запускать программы и просматривать динамически обновляемые данные о производительности компьютера.

Изучив материал этого занятия, Вы сможете:

- ✓ управлять приложениями и задачами при помощи Task Manager;
- ✓ просматривать в Task Manager сведения о производительности системы.

Продолжительность занятия — около 20 минут.

Возможности Task Manager

Task Manager выводит сведения о программах и процессах, выполняющихся в системе. Также утилита отображает наиболее часто используемые счетчики производительности процессов.

Task Manager осуществляет мониторинг ключевых показателей производительности компьютера. Утилита позволяет быстро просмотреть состояние выполняющихся программ и завершить работу приложений, не отвечающих на запросы системы. Помимо этого, Вы можете оценить активность процессов, просмотрев критические частные значения, изучить графики и сведения об использовании процессора и памяти.

Чтобы открыть Task Manager, щелкните правой кнопкой пустое место на панели задач и выберите в контекстном меню команду Task Manager. Кроме того, для запуска Task Manager можно нажать Ctrl+Alt+Del и затем щелкнуть кнопку Task Manager. Интерфейс Task Manager включает три вкладки: Applications (Приложения), Processes (Процессы) и Performance (Быстродействие). Для настройки параметров отображения данных на каждой из вкладок служит меню View (Вид), Перечень его команд зависит от выбранной вкладки.

Для обновления данных Task Manager выберите в меню View команду Refresh Now (Обновить). Вы можете изменить и интервал автоматического обновления данных. В меню View выберите команду Update Speed (Скорость обновления) и щелкните соответствующий пункт. Чтобы временно приостановить вывод данных, в меню View выберите Update Speed, а затем — команду Paused (Приостановить).

Вкладка Applications

На вкладке Applications отображается состояние программ, выполняющихся на компьютере (рис. 13-17). Отсюда можно запустить новое приложение кнопкой New Task (Новая задача), завершить работу программы кнопкой End Task (Снять задачу) или перейти к другому приложению кнопкой Switch To (Переключиться).

Запуск программы из Task Manager осуществляется аналогично запуску программы при помощи меню Start\Run (Пуск\Выполнить). Если программа не реагирует на запросы системы, нажмите Ctrl+Alt+Del, запустите Task Manager, выберите зависшую программу и щелкните кнопку End Task (Снять задачу). Несохраненные данные и изменения будут потеряны.

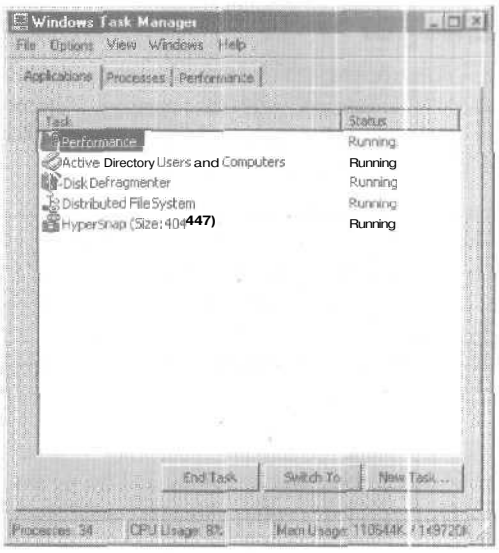


Рис. 13-17. Вкладка Applications (Приложения) утилиты Task Manager

Вкладка **Processes**

На вкладке Processes отображается информация о процессах, выполняющихся в системе (рис. 13-18). Например, здесь можно вывести сведения об использовании памяти и процессора, количестве ошибок памяти, дескрипторов и других параметрах.

На вкладке Processes можно отсортировать список процессов и вывести другие счетчики процессов. Описание доступных счетчиков см. в справочной системе Task Manager. Чтобы вывести список доступных счетчиков процессов, перейдите на вкладку Processes и выберите в меню View (Вид) команду Select Columns (Выбрать столбцы).

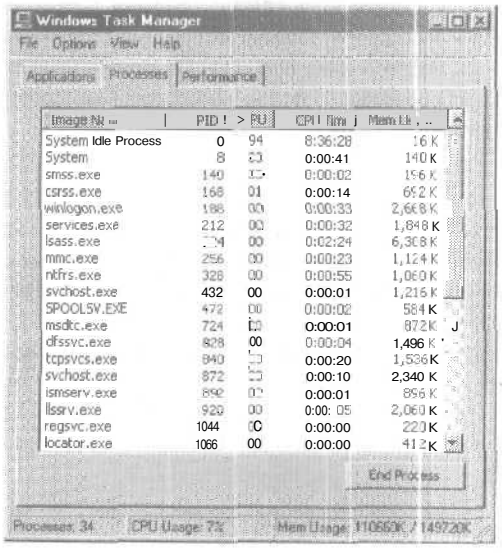


Рис. 13-18. Вкладка Processes (Процессы) утилиты Task Manager

На вкладке Processes можно завершать процессы. При завершении процесса приложения Вы потеряете несохраненные данные. При завершении процесса системной службы некоторая часть системы может работать некорректно.

Примечание Task Manager не позволяет завершать критические процессы Windows 2000. Для этого служат утилиты Windows 2000 Resource Kit, хотя их применение может привести к нестабильной работе системы.

Вы можете завершить процесс и все созданные им процессы. Щелкните требуемый процесс правой кнопкой и выберите в контекстном меню команду End Process Tree (Завершить дерево процессов). Например, если Вы завершите дерево процессов для программы электронной почты, одновременно будут завершены и такие связанные процессы, как mapisp32.exe и спулер MAPI.

На вкладке Processes можно привязывать процесс к процессору командой Set Affinitty, доступной лишь на системах с несколькими процессорами. После выбора процесс будет выполняться лишь на определенных процессорах, что может снизить общую производительность. Помимо этого, вкладка Processes позволяет изменять приоритет выполняющейся программы. В зависимости от назначенного приоритета программа может выполняться быстрее или медленнее; кроме того, она может негативно влиять на производительность других процессов. Если Вы установили отладчик, команда отладки будет доступна в контекстном меню выполняющегося процесса, отображаемого на вкладке Processes.

Вкладка Performance

На вкладке Performance отображаются динамически обновляемые сведения о производительности компьютера (рис. 13-19). Представление включает в себя графики использования процессора и памяти, общее число дескрипторов, потоков и процессов, выполняющихся на компьютере, а также общий объем (в кб) физической памяти, памяти ядра и выделенной памяти.

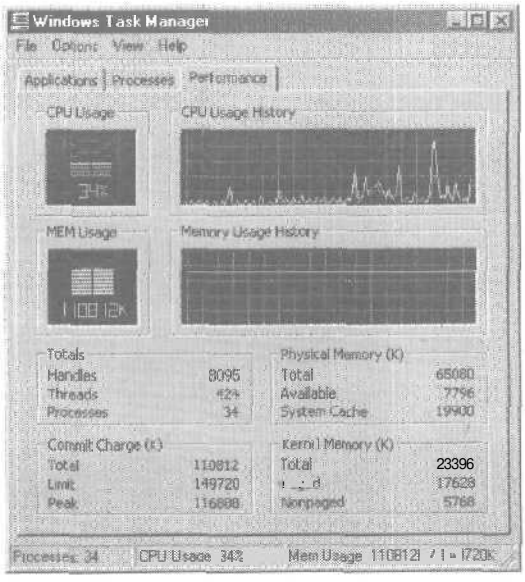


Рис. 13-19. Вкладка Performance (Быстродействие) утилиты Task Manager

Если Вы выберете в меню View команду Show Kernel Times (Вывод времени ядра), в графики CPU Usage (Загрузка ЦП) и CPU Usage History (Хронология загрузки ЦП) добавится красная линия. Она указывает объем ресурсов процессора, используемых операциями ядра.

Резюме

Task Manager выводит сведения о программах и процессах, выполняющихся в системе. Кроме того, утилита отображает наиболее часто используемые счетчики производительности процессов. Интерфейс Task Manager включает три вкладки: Applications (Приложения), Processes (Процессы) и Performance (Быстродействие). На вкладке Applications отображается состояние программ, выполняющихся на компьютере, на вкладке Processes — информация о процессах, а на вкладке Performance — динамически обновляемые сведения о производительности компьютера.

Закрепление материала

Приведенные ниже вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Вы воспользовались утилитой Compact для сжатия файлов подпапки Users на разделе NTFS и пометили флажок Display Compressed Files And Folders With Alternate Color (Отображать сжатые файлы и папки другим цветом). Через неделю Вы решили при помоши Windows Explorer проверить, сжаты ли файлы. Вложенные папки учетных записей пользователей в каталоге Users, созданные после запуска утилиты Compact, оказались несжатыми. Почему это произошло и как решить проблему?

2. Ваш отдел недавно заархивировал несколько гигабайт данных с компьютеров Windows 2000 Server на компакт-диски. После того, как пользователи добавили файлы на сервер, Вы заметили, что время доступа к жесткому диску увеличилось. Как ускорить доступ к диску сервера?

3. Вы администратор компьютера Windows 2000 Server, на котором хранятся домашние каталоги пользователей и перемещаемые профили пользователей. Вам нужно ограничить размер каждого домашнего каталога до 25 Мб и одновременно осуществлять мониторинг, но не ограничивать объем дискового пространства, используемый для хранения перемешаемых профилей. Как настроить тома на сервере?

4. Производительность сервера снизилась. Вам требуется получить суммарную информацию по производительности сервера, и Вы хотите воспользоваться утилитой, которая предоставит подробные сведения об узких местах системы. Что сделать для мониторинга работы сервера по мере роста количества подключенных к нему пользователей после решения проблемы производительности?

5. Вам требуется отфильтровать весь сетевой трафик и выделить трафик между двумя компьютерами; кроме того, Вам надо найти в пакетах определенные данные. Какая функция Network Monitor позволяет это сделать?

6. Ваша цель — гарантировать, что в сети Вашей организации с агентами SNMP могут взаимодействовать лишь 2 станции управления сетью. Как настроить службу SNMP для усиления защиты?

ГЛАВА 14

Серверы приложений Microsoft Windows 2000

В этой главе

Microsoft Windows 2000 Server поддерживает службы, расширяющие функциональные возможности ОС Windows 2000. В этой главе рассказывается о нескольких таких службах, в частности об Internet Information Services (MS), Telnet и Terminal Services. Также здесь содержится информация об их реализации и администрировании в среде Windows 2000.

Прежде всего

Для изучения материалов этой главы необходимо:

- установить Windows 2000 Server на компьютеры Server01 и Server02;
- выполнить упражнения из предыдущих глав.

Занятие 1. Microsoft Internet Information Services 5.0

В Windows 2000 Server входит обновленная, пятая версия служб IIS, которая в своей работе использует службу безопасности и службу каталогов Active Directory. US 5.0 повышает надежность, производительность, безопасность и управляемость Web-сервера, а также расширяет возможности служб приложений. Ниже дается обзор IIS 5.0, описывается процесс его установки и настройки среды Web.

Изучив материал этого занятия, Вы сможете:

- ✓ установить IIS 5.0 и настроить среду Web.

Продолжительность занятия - около 40 минут.

Введение в Microsoft IIS 5.0

IIS 5.0 нацелен на построение Web-узлов, удовлетворяющих требованиям современного бизнеса, все больше ориентирующегося на Интернет и интрасети. Улучшения в 1IS 5.0 коснулись четырех областей: надежности и производительности, управления, безопасности и среды разработки приложений.

Надежность и производительность

IIS 5.0 обладает большей надежностью и производительностью, чем предыдущие версии, по ряду причин. Так, за счет усовершенствования кода была улучшена производительность ядра IIS 5.O. Новая функция перезагрузки позволяет быстро перезапускать сервер. Одно из наиболее существенных улучшений в IIS 5.0 — механизм зашиты приложений посредством пула внепроцессных приложений. Для более эффективного управления ресурсами добавлены функции по ограничению загрузки процессора процессами и ограничению пропускной способности сети для узлов. Кроме того, новая функция *пула сокетов* (Socket Pooling) позволяет нескольким узлам, совместно использующим порт, разделять и набор сокетов.

Защита приложений

Большинство ОС рассматривают процесс как единицу работы в системе. Службы и приложения — это процессы, выполняющиеся в выделенных ОС областях памяти. В [IS 5.0 под защитой приложений понимается механизм защиты памяти, отведенной каждому процессу приложения, от других процессов. В предыдущих версиях IIS все приложения Internet Server API (ISAPI), включая технологию *активных страниц сервера* (Active Server Pages, ASP), совместно использовали ресурсы и память процесса сервера IIS. С одной стороны, это обеспечивало высокую производительность, с другой же — нестабильные компоненты могли вызвать зависание или сбой в работе сервера IIS, что затрудняло разработку и отладку новых компонентов. Кроме того, *процессные компоненты* (in-process components) можно было выгрузить из памяти только путем перезапуска сервера. Это означало, что изменение существующих компонентов затронуло бы все узлы, использующие данный сервер IIS, независимо от того, коснулось их изменение или нет.

Первым шагом в решении этих проблем в IIS 4.0 явилась возможность выполнения приложений как в общем процессе сервера IIS (Inetinfo.exe), так и в отдельных процессах — *внепроцессных* (out-of-process) *приложениях*. В последнем случае для управления каждым приложением используется вспомогательное приложение DLLHost.exe. Внепроцесс-

ные приложения выполняются отдельно друг от друга. Это требует больше памяти и поэтому менее эффективно, чем выполнение приложений в одном процессе. В IIS 5.0 появился третий вариант: приложения могут выполняться в общем процессе, но не в процессе сервера IIS, что позволяет связанным друг с другом приложениям выполняться вместе, не влияя на процесс сервера IIS. Эти три варианта образуют различные уровни защиты, каждый из которых по-своему влияет на производительность. Однако увеличение изоляции процессов снижает производительность.

Перезагрузка

При системном сбое важно быстро восстановить работу IIS. Раньше для перезапуска IIS требовалось перезагрузить компьютер — приемлемое, но не оптимальное решение. Чтобы корректно перезапустить IIS, администратору приходилось использовать четыре разные службы. Это требовало от него специальных знаний, в частности о том, какие службы и в каком порядке нужно запустить. Теперь в этом нет необходимости, так как в Windows 2000 реализована функция безопасной перезагрузки, обеспечивающая более быстрый и гибкий перезапуск, для выполнения которого требуется всего лишь одно действие.

Пул сокетов

IIS 5.0 повышает производительность путем оптимизации доступа к Web-узлу. Сокет – это протокольный идентификатор определенного узла в сети. Он состоит из адреса узла и номера порта, идентифицирующего службу. Например, порт 80 представляет службу World Wide Web HTTP.

В IIS 4.0 каждый Web-узел был связан с собственным IP-адресом, то есть имел собственный сокет, который не мог быть использован другими узлами. Каждый сокет создается при запуске узла и занимает большой объем резидентной памяти. Это ограничивает количество узлов с IP-адресами, которые могут быть созданы на одном компьютере.

В IIS 5.0 узлы, связанные с разными IP-адресами, но совместно использующие один и тот же номер порта, могут совместно использовать и набор сокетов, В результате возросло количество узлов, которые могут быть связаны с одним IP-адресом на том же компьютере. Общие сокеты гибко разделяются между узлами, поэтому ресурсы используются более эффективно.

Размещение нескольких Web-узлов

Для улучшения масштабируемости TIS в Windows 2000 Server поддерживается размещение нескольких Web-узлов на одном сервере. Это позволяет экономить время и деньги организациям и *поставщикам услуг Интернета* (Internet Service Provider, ISP), которым необходимо поддерживать разные узлы для разных отделов или клиентов.

Ключевой вопрос при размещении нескольких Web-узлов на одном сервере — их различение. Это можно сделать несколькими способами, однако все они основаны на применении идентификатора Web-узла. Каждый Web-узел имеет уникальный номер, необходимый для получения запросов и ответов на них, который состоит из номера порта, IP-адреса и имени заголовка хоста. IIS 5.0 позволяет разместить несколько Web-узлов на сервере одним из трех способов: присвоив узлам разные номера портов, разные IP-адреса или разные имена заголовков хостов. У нескольких Web-узлов могут быть две одинаковые характеристики из трех, и тем не менее каждый из них будет уникален.

Примечание IIS 4.0 также позволяет размещать несколько Web-узлов на сервере.

Ограничение процессов

Если у Вас есть несколько Web-узлов, которые используют HTML-страницы, находящиеся на одном компьютере, или на компьютере с Web-сервером выполняются другие прило-

жения, Вы можете ограничить процессорное время, отведенное для выполнения приложений Web-узла. Это позволит выделить достаточное время для обработки других Web-узлов или приложений, не связанных с IIS.

Ограничение пропускной способности

Если сетевое соединение или Интернет-соединение, используемое Web-сервером, также используется другими службами, например службой новостей или электронной почты, Вам, возможно, понадобится ограничить пропускную способность сети, доступную для Вашего Web-сервера, чтобы освободить ее для других служб. IIS 5.0 позволяет регулировать пропускную способность сети для каждого Web-узла, ограничивая доступную пропускную способность сетевого адаптера. При помощи этой функции ISP может, например, выделить каждому узлу заранее определенную пропускную способность.

Примечание IIS 4.0 также позволяет регулировать пропускную способность каждого Web-узла.

Управление

В IIS 4.0 было представлено множество новых технологий. Цель IIS 5.0 — упрощение администрирования Web-сервера. Например, установка IIS 4.0 вызывала трудности у некоторых администраторов, тогда как процесс установки IIS 5.0 встроен в Windows 2000 Server Setup. Кроме того, в IIS 5.0 появилось три новых мастера для облегчения настройки параметров системы безопасности. Были усовершенствованы и административные *сценарии* (scripts), выполняемые из командной строки, и добавлены встроенные сценарии управления.

Интеграция установки и обновления

Установка IIS 5.0 интегрирована в процесс установки Windows 2000 Server — IIS 5.0 устанавливается по умолчанию как один из компонентов ОС. IIS 5.0 обозначен в списке компонентов Windows как Internet Information Services (IIS). Во время установки ОС при помощи мастера компонентов Windows можно установить новую копию IIS 5.0 или обновить старую версию.

При установке Windows 2000 Server автоматически создаются узлы Default Web site (Веб-узел по умолчанию) и Administration Web site (Администрирование веб-узла), а также Default SMTP Virtual Server (Виртуальный SMTP-сервер по умолчанию). При помощи приложения Add/Remove Programs из окна Control Panel можно добавить или удалить US или его дополнительные компоненты, например, службу NNTP. Для этого дважды щелкните значок Add/Remove Programs и в открывшемся окне щелкните кнопку Add/Remove Windows Components (Установка и удаление компонентов Windows). В списке компонентов выберите Internet Information Services (IIS) и щелкните кнопку Details (Состав).

Централизованное администрирование

IIS 5.0 управляется при помощи оснастки Internet Information Services (рис. 14-1), интегрированной с другими административными функциями Windows 2000. (В предыдущих версиях этот инструмент назывался Internet Service Manager.) Оснастку Internet Information Services можно вызвать из программной группы Administrative Tools или запустить из узла Services and Applications (Службы и приложения) оснастки Computer Management.

Основанное на интерфейсе браузера средство администрирования Internet Services Manager (HTML) теперь недоступно из программной группы Administrative Tools (Администрирование). Оно сохранено для возможности удаленного администрирования IIS через соединения HTTP или HTTPS (в зависимости от параметров безопасности Web-узла

администрирования). Для вызова Internet Services Manager (HTML) в оснастке Internet Information Services щелкните папку Administration Web Site (Администрирование веб-узла), а затем в меню Action (Действие) выберите команду Browse (Обзор). Его можно вызвать и из окна браузера, указав в поле адреса имя сервера, присвоенный узлу номер порта TCP и адрес Web-узла Administration (рис. 14-2).

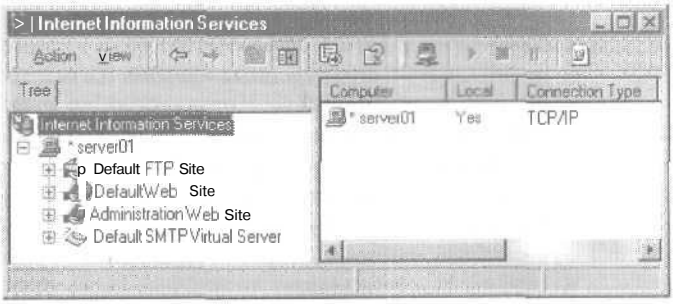


Рис. 14-1. Оснастка Internet Information Services

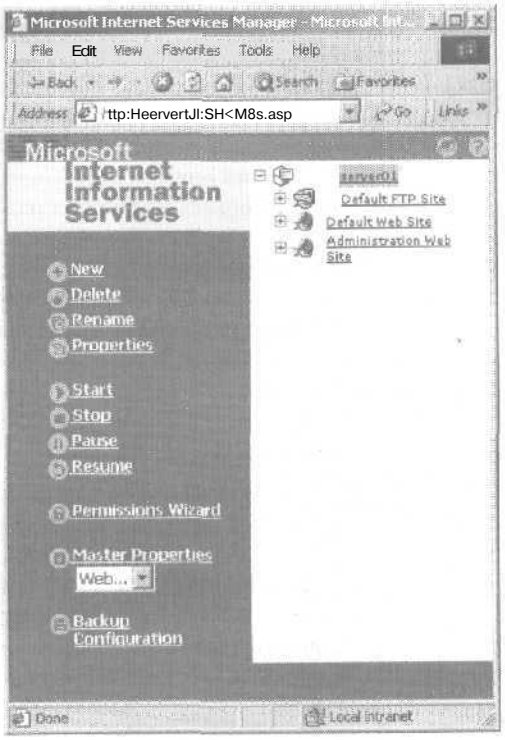


Рис. 14-2. Администрирование IIS на Server01 с удаленногокомпьютера

Примечание Номер порта TCP, присваиваемый административному узлу, выбирается случайным образом из чисел от 2000 до 9999. Чтобы узнать или изменить этот номер, откройте диалоговое окно свойств Web-узла Administration и перейдите на вкладку Web Site (Веб-узел).

Для доступа к административному узлу можно использовать не только Microsoft Internet Explorer, но и другие браузеры (обозреватели). Если обозреватель не поддерживает аутентификацию NTLM и Вы не хотите разрешать анонимный доступ, включите базовую аутентификацию. Для удаленного администрирования IIS при помощи оснастки Internet Information Services можно использовать и службы Terminal Services.

Делегированное администрирование

Для распределения нагрузки по управлению можно добавить административные учетные записи в группу Operators. Члены этой группы имеют ограниченные административные привилегии в отношении Web-узлов. Например, поставщик услуг Интернета, размещающий узлы множества организаций, может назначить представителей каждой организации операторами соответствующего Web-узла. Операторы могут управлять параметрами, относящимися только к узлам, находящимся в их компетенции. У них нет доступа к параметрам, определяющим работу IIS в целом, компьютера-сервера с Windows, на котором установлен IIS, или сети. Это избавляет системного администратора поставщика услуг Интернета, поддерживающего несколько Web-узлов на одном сервере, от повседневного управления Web-узлами, при этом не отнимая у него общих административных полномочий.

Учет процессов

Новая функция IIS 5.0 — *учет процессов* (process accounting) — позволяет администратору отслеживать использование Web-узлами ресурсов процессора сервера и сохранять эту информацию в журнал. Учет процессов добавляет поля в файл журнала W3C Extended. С помощью этой информации поставщик услуг может выявить узлы, занимающие непропорционально большую долю ресурсов процессора, а также узлы со сценариями или процессами CGI (Common Gateway Interlace), содержащими ошибки. Эта информация может понадобится специалистам отдела автоматизации, чтобы сбалансировать затраты на размещение Web-узла или приложения.

Чтобы активизировать учет процессов для узла с помощью оснастки Internet Information Services, откройте окно свойств узла, затем окно свойств W3C Extended Log File Format (Расширенный формат файла журнала W3C) и перейдите на вкладку Extended Properties (Расширенные свойства). Затем произведите те же операции в окне Internet Service Manager (HTML) и щелкните ссылку Extended Properties. На рис. 14-3 изображено диалоговое окно Extended Logging Properties и Web-страница Extended Logging Options,

Усовершенствованные административные сценарии, выполняемые из командной строки

В комплект IIS 5.0 входят сценарии для автоматизации управления типичными заданиями Web-сервера. Они находятся в папке \Inetpub\Scripts и могут быть вызваны из командной строки. Административные сценарии служат для автоматизации наиболее типичных административных задач: создание и управление Web-узлами, приложениями, каталогами и пр. Администраторы могут также создавать собственные сценарии, автоматизирующие управление IIS. Выполнение административных сценариев с расширением .vbs, входящих в MS 5.0, осуществляется при помощи сервера сценариев Windows — Windows Script Host (WSH).

Архивирование и восстановление IIS

Оснастка Internet Information Services позволяет архивировать и восстановливать конфигурацию IIS, то есть сохранять параметры метабазы IIS 5.0, чтобы иметь возможность вернуться в известное и безопасное состояние. Это позволяет архивировать и восстанавливать конфигурацию Web-сервера, но не файлы содержимого или параметров в реестре.

Для архивирования и восстановления конфигурации Web-сервера в дереве консоли щелкните Internet Information Services, а затем в меню Action (Действие) выберите коман-

ду Backup/Restore Configuration (Архивирование и восстановление конфигурации). Откроется диалоговое окно Configuration Backup/Restore (Архивирование/восстановление конфигурации), где можно создать архивную копию, восстановить конфигурацию из архива или удалить ранее созданный архив (рис. 14-4).

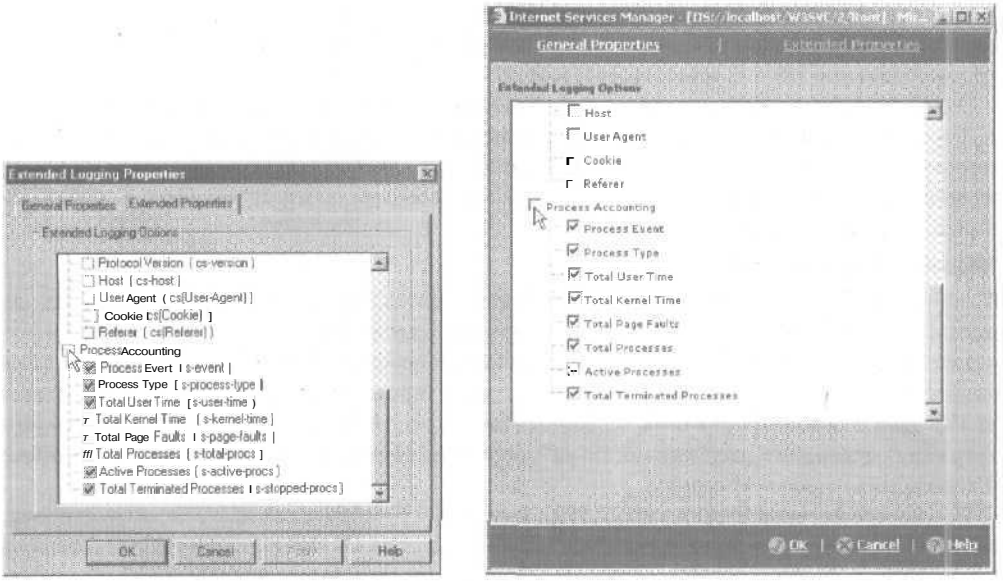


Рис. 14-3. Активизация учета процессов из диалогового окна Extended Logging Properties (Расширенные свойства ведения журнала) или с Web-страницы Extended Logging Options (Расширенные параметры ведения журнала)

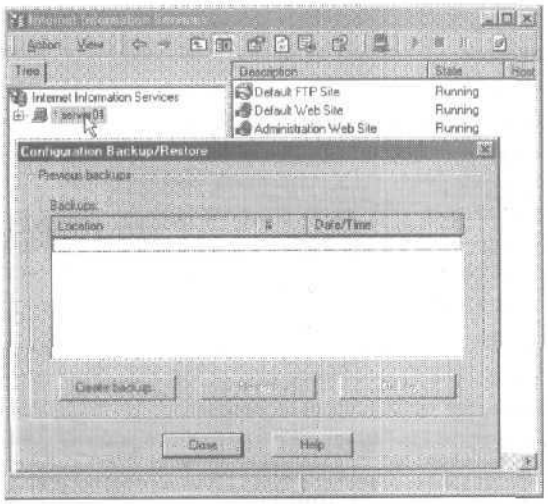


Рис. 14-4. Диалоговое окно Configuration Backup/Restore (Архивирование/восстановление конфигурации)

Нестандартные сообщения об ошибках

Если при пользовательском соединении с Web-узлом возникает ошибка HTTP, то на клиентский браузер посылается базовое сообщение об ошибке с кратким описанием того, что произошло при попытке установить соединение. Подобно IIS 4.0, 1IS 5.0 позволяет посылать клиентам более содержательные сообщения при возникновении ошибок в коде ASP- или HTML-страниц на узле. Вы можете выбрать нестандартное сообщение об ошибке, предоставляемое IIS 5.0, или создать свое.

В IIS 5.0 нестандартные сообщения об ошибках хранятся в папке %systemroot%\Help\iisHelp\common, а в IIS 4.0 — в папке %systemroot%\Help\common. Файл с сообщением об ошибке имеет расширение .htm, а его имя совпадает с именем ошибки. Если в сообщении об ошибке содержится точка, например, 403.3, то в имени соответствующего файла вместо нее будет стоять дефис (403-3.htm).

Поддержка серверных расширений FrontPage

Windows 2000 Server позволяет администраторам использовать инструменты FrontPage для создания и управления Web-узлами. При помощи серверного расширения FrontPage администраторы могут просматривать Web-узлы и управлять ими, используя графический интерфейс, а авторы — удаленно создавать, редактировать и публиковать Web-страницы на IIS. Для администрирования серверных расширений FrontPage и Web-узлов, поддерживающих серверные расширения FrontPage, служит оснастка FrontPage Server Extensions (Расширения сервера Microsoft).

В отличие от предыдущих версий IIS в версии 5.0 FrontPage служба Web активизирована по умолчанию. К модулю FrontPage Server Extensions можно перейти либо из консоли Server Extensions Administrator, либо из оснастки Internet Information Services. FrontPage Server Extensions содержит две функции, играющие важную роль при первоначальной настройке и проверке расширений:

- **настройка существующего Web-сервера на использование серверных расширений** позволяет работать с ним Web-приложениям, зависящим от серверных расширений (например FrontPage);
- проверка **безопасности серверных расширений** позволяет проверять безопасность всех или одного Web-узла с серверными расширениями.

Чтобы настроить Web-сервер на использование серверных расширений, в оснастке Internet Information Services выберите Web-узел, в меню Action (Действие) — New (Создать), а затем — команду Server Extensions Web (Web-узел серверных расширений). Для проверки безопасности серверных расширений всех Web-узлов в дереве консоли щелкните Internet Information Services, в меню Action — All Tasks (Создать), а затем — команду Check Server Extensions (Проверить серверные расширения). Для проверки серверных расширений только на одном узле выберите имя этого узла в дереве консоли и выполните те же процедуры, что и при проверке всех узлов.

Распределенные авторские версии

Хотя Web является превосходным средством для публикации документов, до недавнего времени организациям было нелегко использовать Интернет для совместной работы с документами, потому что внести изменения в документы, хранящиеся на Web-узле, в отличие от их чтения было достаточно сложно. Для решения этой проблемы в IIS 5.0 была добавлена поддержка распределенных авторских версий (WebDAV).

Установив каталог WebDAV на Web-сервере, Вы откроете пользователям совместный доступ к документам через Интернет или интрасеть. WebDAV в IIS 5.0 эффективно использует возможности защиты и управления доступом к файлам, предоставляемые Win-

dows 2000. Это позволяет устанавливать и снимать блокировки на ресурсы, чтобы несколько пользователей могли читать файл, а вносить в него изменения одновременно мог бы только один пользователь. Подробности о WebDAV см. в занятии 2 этой главы.

Распределенная файловая система

IIS 5.0 использует *распределенную файловую систему* (distributed file system, DFS) WinJows 2000, которая позволяет объединить файлы, хранящиеся на различных компьютерах, в единое пространство имен. При помощи DFS системные администраторы могут построить единую иерархическую структуру из файлов, хранящихся на различных файловых серверах, облегчая пользователям доступ и управление файлами, физически расположенными в разных частях сети. Эту структуру можно организовать так, что файлы, расположенные на нескольких серверах, будут казаться пользователям хранящимися в одном месте в сети. Поэтому для доступа к файлам пользователям не нужно будет знать и указывать их физическое расположение.

Примечание Подробнее о DFS см. занятие 1 главы 5.

Сжатие HTTP

В зависимости от содержания, объема дискового пространства и скорости передачи данных типичного посетителя сервера сжатие HTTP может обеспечить более быструю передачу страниц между Вашим Web-сервером и обозревателем Web , поддерживающим получение сжатой информации. Это полезно, котда пропускная способность сети ограничена.

Для включения режима сжатия HTTP в окне свойств папки Internet Information Services щелкните кнопку Edit (Изменить) для WWW Service (WWW-служба) и в открывшемся окне перейдите на вкладку Service (Служба) (рис. 14-5).

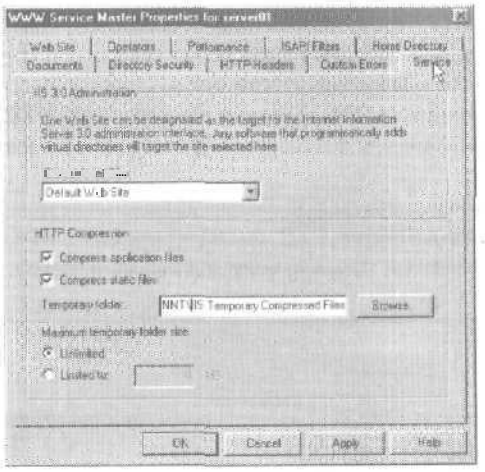


Рис. 14-5. Диалоговое окно WWW Service Master Properties for Server01 (Основные свойства WWW-службы для ServerOl) в оснастке Internet Information,Services

На домашней странице Internet Information Service (HTML) щелкните ссылку Master Properties (Основные свойства), а затем — ссылку Service (Служба). Просмотрите служебные свойства и при необходимости настройте сжатие (рис. 14-6).

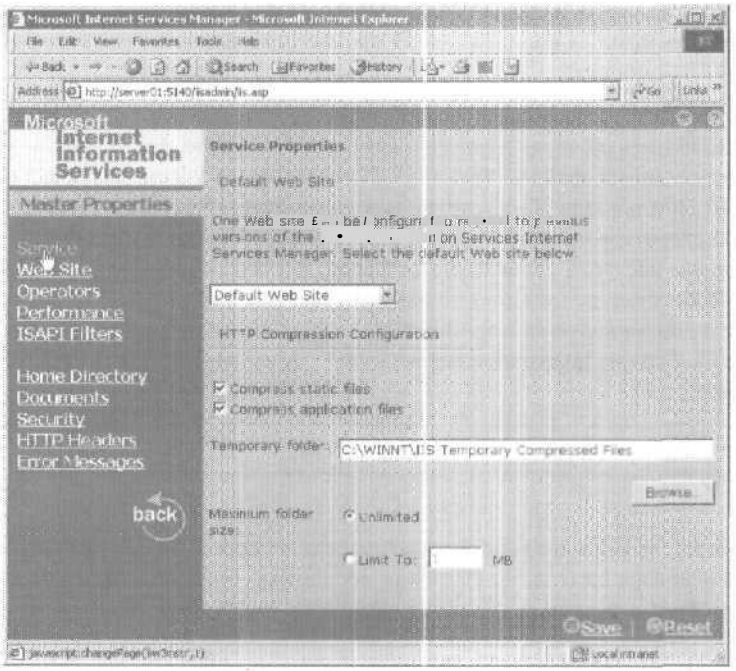


Рис. 14-6. Web-страница **Service Properties (Свойства службы)**

Протоколы FTP и FTP Restart

В Windows 2000 Server интегрирован протокол FTP, являющийся промышленным стандартом для публикации информации на Web-сервере, Windows 2000 Server также поддерживает протокол FTP Restart, входяший в IIS 5.0 и обеспечивающий быструю и удобную загрузку информации из Интернета. При прерывании сеанса передачи данных с узла FTP можно не производить повторную загрузку всего файла, а дозагрузить его с места обрыва соединения.

Примечание Эта функция доступна только для клиентов FTP, поддерживающих дозагрузку по протоколу FTP. Для повторного соединения и продолжения прерванной загрузки клиент FTP выполняет команду REST.

Безопасность

В IIS 5.0 значительно улучшена система безопасности. Она использует преимущества стандартов безопасности Интернет, полностью поддерживаемых Windows 2000.

Стандарты безопасности

В таблице приведены протоколы безопасности, поддерживаемые IIS 5.O.

Стандарт безопасности	Описание
Fortezza	IIS 5.0 поддерживает американский правительственный стандарт безопасности Fortezza. Он удовлетворяет архитектуре безопасности Defense Message System, поддерживая механизм шифрования, обеспечивающий конфиденциальность, целостность и подлинность сообщений, аутентификацию, контроль доступа к сообщениям, компонентам и системам. Эти функции реализуются как при помощи ПО сервера и браузера, так и при помощи аппаратных средств — платы PCMCIA.
Secure Sockets Layer (SSL) 3.0	Протоколы безопасности SSL широко используются Web-браузерами и серверами для аутентификации, конфиденциальности и целостности сообщений. При помощи функций безопасности SSL можно проверить целостность содержания Вашего Web-сервера, реквизиты пользователей и шифровать передаваемые по сети сообщения. SSL основаны на сертификатах, создаваемых с помощью Microsoft Certificate Services. (О сертификатах и Certificate Services см. также занятие 1 главы 11.)
Transport Layer Security (TLS)	TLS основан на SSL. Он помогает выполнять безопасную аутентификацию пользователей, а независимым программистам позволяет создавать поддерживающий TLS код, способный обмениваться зашифрованной информацией с другим процессом без ознакомления с кодом, созданным другим программистом. Кроме того, TLS является каркасом для построения новых методов шифрования с открытым ключом и шифрования больших объемов данных. TLS служит и для повышения производительности, уменьшая сетевой трафик и предлагая схему кэширования сессий, позволяющую сократить количество соединений, устанавливаемых «с нуля*.
PKCS #7	Этот протокол описывает формат зашифрованных данных, например цифровых подписей или цифровых конвертов.
PKCS #10	Этот протокол описывает формат посылаемых сертификационным центрам (Certificate Authority CA) запросов на получение сертификата.
Обычная проверка подлинности	Обычная аутентификация — стандартный метод сбора информации об именах пользователей и паролях. Она посылает пароли по сети в формате Base64 Encoded. К ее достоинствам можно отнести то, что она является частью спецификации HTTP 1.0 и поэтому поддерживается большинством браузеров. Однако обычная аутентификация имеет существенный минус — использующие ее Web-браузеры пересылают пароли в незашифрованном виде. Это позволяет хакеру перехватить и расшифровать их. Поэтому, если Вы не уверены в безопасности соединения между пользователем и Вашим Web-сервером (безопасным может считаться прямое кабельное соединение, выделенная линия или безопасное соединение интрасети), применять обычную аутентификацию не рекомендуется.

(*окончание*)

Стандарт безопасности	Описание
Краткая проверка подлинности	В IIS 5.0 появился новый механизм аутентификации — краткая аутентификация. Она обладает теми же возможностями, что и обычная, но передает аутентификационные сведения иначе. Они проходят через одношаговый процесс — *хеширование* (hashing). Результат этого процесса называется *хешем* (hash), или *выборкой сообщения* (message digest). Исходный текст ни может быть расшифрован из хеша. Перед хешированием к паролю добавляется дополнительная информация, генерируемая сервером, поэтому никто не сможет перехватить хеш пароля и с его помощью выдавать себя за истинного клиента. Краткая аутентификация основана на методологии общего секретного пароля. Она имеет неоспоримое преимущество перед обычной аутентификацией, где пароль может быть перехвачен и несанкционированно использован. Краткая аутентификация структурирована для использования несколькими прокси-серверами и другими брандмауэрными приложениями, а также доступна в WebDAV. Так как краткая аутентификация является новой возможностью HTTP 1.1, она поддерживается не всеми обозревателями. Если не поддерживающий краткую аутентификацию браузер пошлет запрос на сервер, требующий именно этот способ аутентификации, сервер не будет обрабатывать запрос и сообщит клиенту об ошибке. Краткая аутентификация доступна только для доменов Windows 2000. Одним из немногих браузеров, поддерживающих эту возможность, является Internet Explorer 5 или более поздней версии.
Встроенная проверка подлинности	Обеспечивает аутентификацию NTLM (Windows NT Challenge/Response) для ранних версий Internet Explorer, использующих ее для криптографической аутентификации в IIS. Для Web-узлов и новых Windows версий Internet Explorer встроенная аутентификация Windows обеспечивает аутентификацию Kerberos v5 и используется, только если вследствие разрешений TFS анонимный доступ запрещен или пользователю отказано в анонимном доступе. Не поддерживается при соединениях с прокси-сервером.

Механизмы безопасности

Путем проверки подлинности Вы можете удостовериться в личности каждого клиента, запрашивающего доступ к вашим Web-узлам. IIS поддерживает для служб HTTP и FTP:

- анонимную проверку подлинности HTTP и FTP;
- обычную проверку подлинности HTTP и FTP;
- краткую проверку подлинности для доменов Windows 2000 и браузеров, поддерживающих этот способ аутентификации, реализованный в HTTP 1.1;
- интегрированную проверку подлинности Windows (только HTTP).

Сертификаты

Для завершения аутентификации нужен механизм проверки реквизитов пользователей. Сертификаты — это цифровые идентификационные документы, позволяющие серверам и клиентам устанавливать подлинность друг друга. Сертификаты необходимы серверу и клиентскому браузеру для установления соединения SSL, по которому посылается зашифро-

ванная информация. Сертификат сервера обычно содержит сведения о Вашей компании и об организации, выпустившей сертификат, а сертификат клиента — информацию, идентифицирующую пользователя и выпустившую сертификат организацию.

Управление доступом

Установив подлинность пользователя, Вы, возможно, захотите управлять его доступом к ресурсам сервера. В IIS 5.0 используется два уровня контроля доступа: разрешения Web и разрешения NTFS. Первые распространяются на все клиенты HTTP и определяют доступ к ресурсам сервера. Вторые определяют уровень доступа индивидуальных учетных записей пользователя к папкам/файлам сервера.

Шифрование

Помимо управления доступом к информации, необходимо защищать эту информацию при передаче ее через Интернет. Пользователи могут осуществлять безопасный обмен с Вашим сервером личной информацией (например номерами кредитной карты или телефона) с помошью шифрования. В этом случае информация зашифровывается перед отправлением и расшифровывается по получении. Шифрование основано на протоколе SSL 3.0 и на новом протоколе TLS 1,0, обеспечивающем шифрованное соединение с пользователями. SSL проверяет подлинность Вашего Web-узла и пользователей, обращающихся к Web-узлам с ограниченным доступом (последнюю функцию можно включать и отключать).

Аудит

Заключительный шаг в обеспечении безопасности — регулярное отслеживание использования вашего узла. С помощью аудита безопасности администраторы могут осуществлять всестороннее наблюдение за системой безопасности Web-сервера и действиями пользователей. Аудит заключается в создании политик аудита доступа к файлам и каталогам и событий сервера, а также в просмотре журналов безопасности для обнаружения попыток несанкционированного доступа. Подробнее об аудите см. занятие 5 главы 13.

Мастеры безопасности

Для облегчения процесса создания и настройки параметров безопасности в IIS 5.0 включены три новых мастера безопасности: Web Server Certificate (Мастер сертификатов веб-сервера), Permissions (Мастер разрешений) и Certificate Trust Lists (Мастер списка доверенных сертификатов).

Мастер сертификатов (рис. 14-7) упрощает выполнение таких административных задач, как создание запросов на сертификаты или управление жизненным циклом сертификатов. Для его запуска щелкните кнопку Server Certificate (Сертификат) в окне свойств Web-узла оснастки Internet Information Services.

Поддержка безопасности SSL стала обычным требованием к коммерческим Web-узлам. При помощи нового мастера стало очень просто создать поддерживающий SSL Web-узел на компьютере с Windows 2000 Server. Кроме того, этот мастер облегчает установку и поддержку шифрования SSL, а также проверку подлинности клиентских сертификатов.

Мастер разрешений позволяет администраторам настроить разрешения и аутентификацию доступа к Web-узлу IIS, облегчая задачу управления Web-узлом, требующим аутентификации для доступа к своему содержанию.

Для запуска мастера разрешений выберите Web-узел или узел FTP в оснастке Internet Information Services, в меню Action (Действие) — All Tasks (Все задачи), а затем — команду Permissions wizard (Мастер разрешений). На рис. 14-8 показано окно мастера разрешений, запущенного из оснастки Internet Information Services.

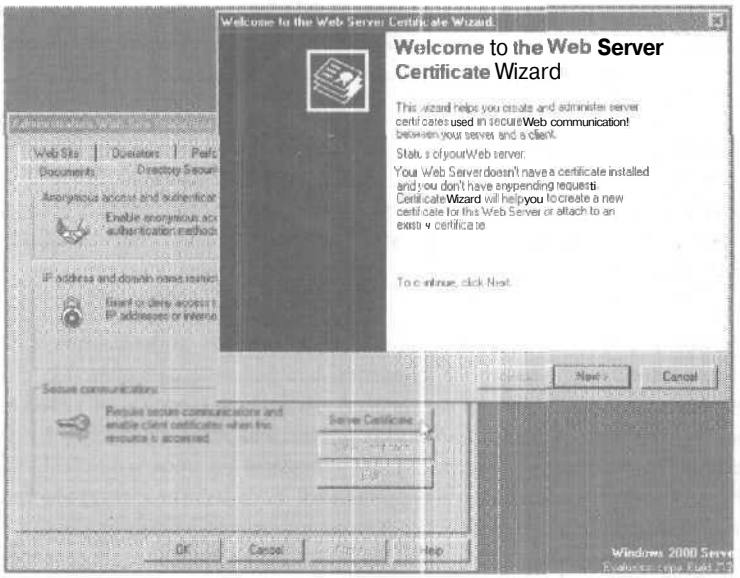


Рис. 14-7, Запуск мастера Web Server Certificate (Мастер сертификатов веб-сервера) из окна свойств узла Administration (Администрирование)

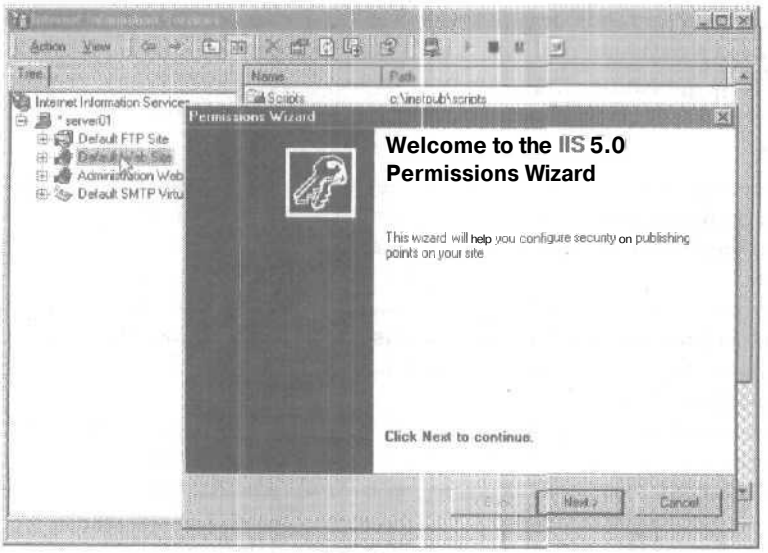


Рис. 14-8. Окно мастера Permissions (Мастер разрешений)

Мастер разрешений можно запустить и из диспетчера Internet Services Manager (HTML) — на его домашней странице выберите Web- или FTP-узел и щелкните ссылку Permissions Wizard (Мастер разрешений) (рис. 14-9).

В мастере разрешений настраиваются два параметра верхнего уровня:

- наследование параметров безопасности от родительского узла или виртуального каталога;
- применение параметров безопасности на основе шаблона.

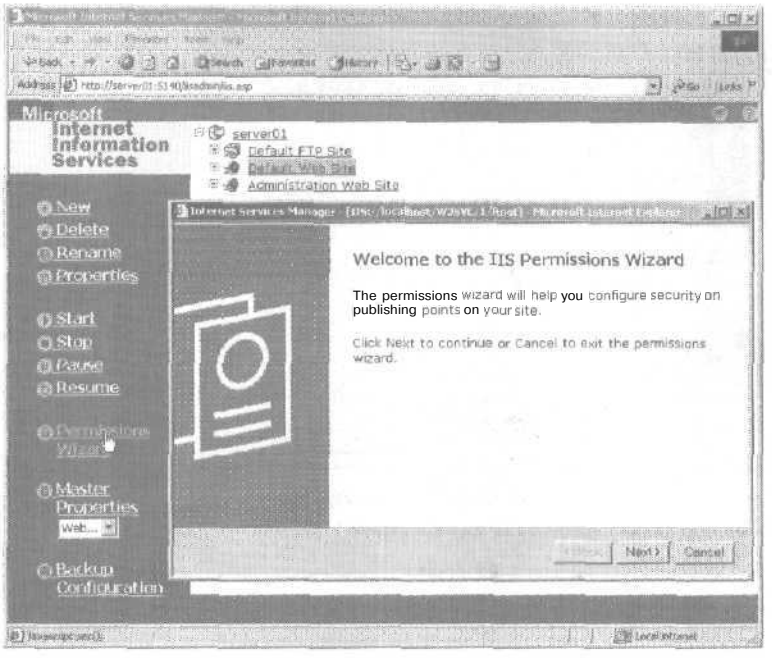


Рис. 14-9. HTML-версия мастера разрешений

Для настройки системы безопасности предусмотрены шаблоны Public Web Site и Secure Web Site. Шаблон Public Web Site содержит установки безопасности, которые, во-первых, поддерживаются различными браузерами, во-вторых, не требуют наличия учетной записи Windows 2000 для доступа к узлу. При применении параметров из шаблона Secure Web Site доступ к узлу разрешается только пользователям, имеющим учетную запись Windows 2000.

Мастер Certificate Trust List используется администраторами для настройки *списков доверия сертификатов* (certificate trust list, CTL). CTL — это список пользующихся доверием сертификационных центров для определенного каталога. Эти списки особенно полезны для поставщиков услуг, которые размещают несколько Web-узлов на своих серверах и которым необходимо иметь отдельный список пользующихся доверием сертификационных центров для каждого узла. CTL доступны только на уровне Web-узлов; для узлов FTP они недоступны.

Мастер Certificate Trust List можно запустить только после того, как Web-узел был настроен с помощью мастера сертификатов сервера. Для запуска этого мастера в оснастке Internet Information Services откройте диалоговое окно свойств Web-узла, перейдите на вкладку Directory Security (Безопасность каталога) и щелкните кнопку Edit (Изменить) в группе Secure Communications (Безопасные подключения). В открывшемся диалоговом окне пометьте флажок Enable certificate trust list (Включить список доверенных сертификатов) и щелкните кнопку New (Создать) — откроется окно мастера Certificate Trust List (рис. 14-10).

Активизация и настройка CTL возможна и из диспетчера Internet Services Manager (HTML), хотя мастер там и не предусмотрен. Кроме того, с помощью оснастки Internet Information Services вы можете редактировать сертификаты, тогда как через интерфейс HTML этого не сделать.

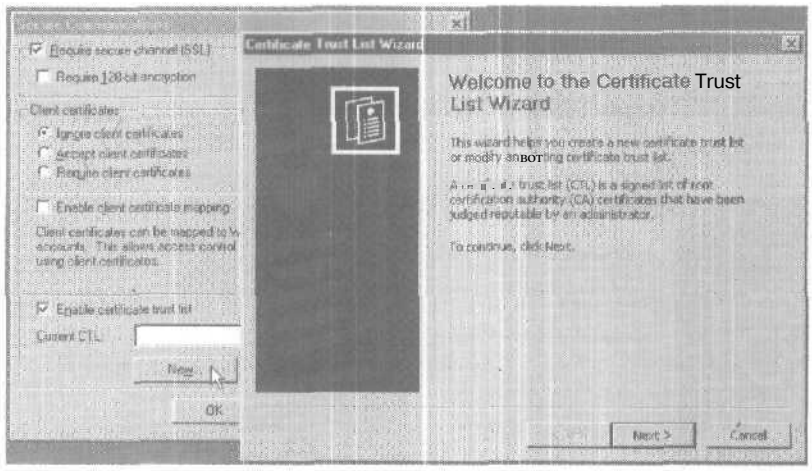


Рис. 14-10. Вызов мастера Certificate Trust List (Мастер списка доверенных сертификатов) после активизации CTL

Среда приложений

В I1S 5.0 улучшена производительность, что облегчило процесс разработки Web-приложений. Входящая в IIS технология ASP в сочетании со службами доступа к данным и службами компонентов Windows 2000 Server формирует полноценную среду приложений.

Такие новинки Windows 2000, как улучшенные управление потоками и обработка ошибок, компоненты WSH и др., упрощают разработку сценариев и Web-приложений с помощью ASP. Кроме того, благодаря использованию ASP без сценариев, автонастройке ASP и более эффективных объектов, а также улучшениям в ОС Windows 2000, ускорилось выполнение приложений ASP,

ASP — это среда для разработки сценариев на стороне сервера, при помощи которой можно создавать и выполнять динамические интерактивные приложения для Web-сервера. Используя ASP, Вы можете создавать на основе страниц HTML, команд сценариев и компонентов *модели компонентных объектов* (Component Object Model, COM), легко внедряемые и модифицируемые интерактивные Web-страницы и Web-приложения. Ряд новинок IIS 5.0, одни из которых (например управление потоками и обработка ошибок) облегчают написание и управление поведением Web-приложений, а другие (ASP без сценариев) увеличивают производительность ASP-страниц.

Службы компонентов

Входящие в Windows 2000 Server IIS 5.0 и службы компонентов (COM+) формируют основу архитектуры для построения Web-приложений. В версии IIS 4,0 поддержку транзакций обеспечивал Microsoft Transaction Server (MTS). В IIS 5.0 и Windows 2000 поддержка транзакций, а также ряд других функций, касающихся разработки и внедрения компонентов, обеспечивается Component Services. Используя их, IIS:

- организует приложения в виде отдельных процессов;
- управляет взаимодействием между компонентами COM (включая встроенные объекты ASP);
- координирует транзакции для ASP-приложений, использующих транзакции.

Службы Active Directory

Хранят и управляют информацией о сетевых ресурсах и формируют центральное хранилище наиболее важной информации, что упрощает сетевое администрирование, поиск ресурсов и разработку приложений.

Интерфейсы Microsoft Active Directory Service Interfaces (ADSI) — основанная на COM модель службы каталогов, позволяющая ADSI-совместимым клиентским приложениям обращаться к разным службам каталогов через единый набор интерфейсов. Разработчикам клиентских приложений не нужно вникать в подробности реализации и функционирования лежащих в основе приложения хранилищ данных и протоколов.

Основная информация по настройке Интернет-узла хранится в метабазе IIS. Для доступа приложений к метабазе и управления ею в 1IS имеется низкоуровневый интерфейс DCOM, а также ADSI-поставщик, который содержит большинство функций DCOM и может быть использован любыми ADSI-совместимыми клиентскими приложениями.

Примечание О новых возможностях IIS 5.0 см. документ \chapt14\articles\IISover.doc на прилагаемом компакт-диске.

Установка IIS 5.0

Internet Information Services 5.0 является одним из компонентов ОС Windows 2000. Установку и удаление IIS можно осуществить одним из трех способов: установив или обновив Windows 2000, с помощью утилиты Add/Remove Programs в Control Panel или указав соответствующие параметры в файле unattended.txt при автоматической установке.

При установке Windows 2000 Server на чистый жесткий диск IIS 5.0 устанавливается по умолчанию. Для удаления IIS и установки/удаления компонентов IIS служит утилита Add/Remove Programs.

При обновлении до Windows 2000 предыдущих версий Windows программа Setup ищет предыдущие версии IIS, Peer Web Services или Personal Web Server. При обнаружении хотя бы одной из этих программ происходит установка IIS 5.0, которую нельзя запретить. Если же ни одна из этих программ у Вас не установлена, I1S 5.0 также не будет установлена.

При установке IJS 5.0 (как на чистый жесткий диск, так и при обновлении) Setup проверяет наличие набора протоколов TCP/IP. При его отсутствии происходит его автоматическая установка и настройка для использования DHCP.

Во время установки IIS 5.0 создаются Web-узлы Default (Веб-узел по умолчанию) и Administration (Администрирование веб-узла), FTP-узел Default (FTP-узел по умолчанию), а также сервер Default SMTP Virtual Server (Виртуальный SMTP-сервер по умолчанию). Об управлении Web- и FTP-узлами см. занятие 2 этой главы.

Примечание Работа с Default SMTP Virtual Server здесь не рассматривается. Протокол SMTP обеспечивает доставку электронной почты в интрасетях и Интернете.

Настройка среды Web

Принципы предоставления материала Web-узла пользователям одинаковы и в Интернете, и в интрасетях. Web-файлы помешаются в папки Вашего сервера, после чего, установив соединение HTTP, пользователи могут просматривать эти файлы при помощи свои> Web-браузеров. Однако для организации узла недостаточно просто хранить файлы на сервере. Вы должны также управлять развертыванием Вашего узла и, что наиболее важно, его развитием.

Начальные действия

Для создания Web-узла нужно указать папки, в которых будут храниться публикуемые документы. Web-сервер не может публиковать документы, находящиеся вне этих папок. Так что в первую очередь при развертывании Web-узла надо организовать структуру хранения файлов. Затем из оснастки Internet Information Services или интерфейса Internet Services Manager (HTML) следует указать, какие папки являются частью Web-узла (в оснастке Internet Information Services и интерфейсе HTML вместо папки используется термин *каталог).*

Если Вы не хотите опубликовать файлы, не тратя времени на организацию специальной структуры папок, и все файлы находятся на жестком диске компьютера с IIS, скопируйте их в домашнюю папку. Пользователи интрасети могут обращаться к этим файлам по одному из следующих URL:

- http://<*имя_компьютера/имя_файла*>;
- http://<*полное_доменное_имя/имя_файла*>;
- http://< *IP-адрес/имя_файла*>,

где *имя_компьютера*, *полное_доменное_имя* и *IP-адрес* идентифицируют Web-сервер.

Примечание В следующем разделе вместо термина *папка* (folder) употребляется термин *каталог* (directory), так как именно он используется в интерфейсе IIS.

Задание домашних каталогов

Каждый Web-узел и FTP-узел должен иметь свой домашний каталог. Это отправная точка для хранения публикуемых страниц на Web-узле. В нем находится домашняя страница (обычно называемая index.htm, index.html, default.asp, default.htm или default.html), приветствующая пользователей Web-браузеров и содержащая ссылки на другие страницы узла. Для одного узла можно указать несколько стартовых страниц. При этом будет отображаться та страница, которую MS найдет первой. Домашний каталог привязывается к доменному имени узла или к имени Вашего сервера. Например, если доменное имя узла - www.microsoft.com, а имя домашнего каталога — C:\Website\Microsoft, то для доступа к файлам из домашнего каталога браузеры будут использовать URL *http://www.microsoft.com.* Если Вы работаете в интрасети и Ваш сервер имеет имя AcctServer, для доступа к файлам в Вашем домашнем каталоге будет применяться URL *http://acctserver.*

Домашний каталог создается по умолчанию при установке IIS и при создании нового Web-узла. Если Вы создаете на одном компьютере узлы WWW и FTP, то для них надо задать различные домашние каталоги. По умолчанию домашним каталогом для службы WWW является \InetPub\Wwwroot, а для службы FTP — \InetPub\Ftproot, но в качестве домашнего каталога можно выбрать и другой.

Чтобы изменить домашний каталог, откройте оснастку Internet Information Services, выберите нужный Web- или FTP-узел и откройте диалоговое окно его свойств. Перейдите на вкладку Home Directory (Домашний каталог) и укажите расположение Вашего домашнего каталога (рис. 14-11).

Если в качестве дочашнего каталога задан общий сетевой каталог, для доступа к нему понадобится ввести имя пользователя и пароль. Для этого рекомендуется использовать учетную запись IUSR_*имя_ компьютера.* Если Вы используете учетную запись с административными полномочиями, клиенты получат доступ к управлению сервера, что поставит под угрозу безопасность вашей сети.

Домашний каталог может располагаться на компьютере с IIS, быть общим сетевым ресурсом или находиться на другом Web-узле (в этом случае доступ к нему осуществляет-

ся путем переадресации по соответствующему URL). Выбрав в качестве домашнего каталога разделяемый сетевой ресурс, Вы можете в полной мере использовать средства DFS.

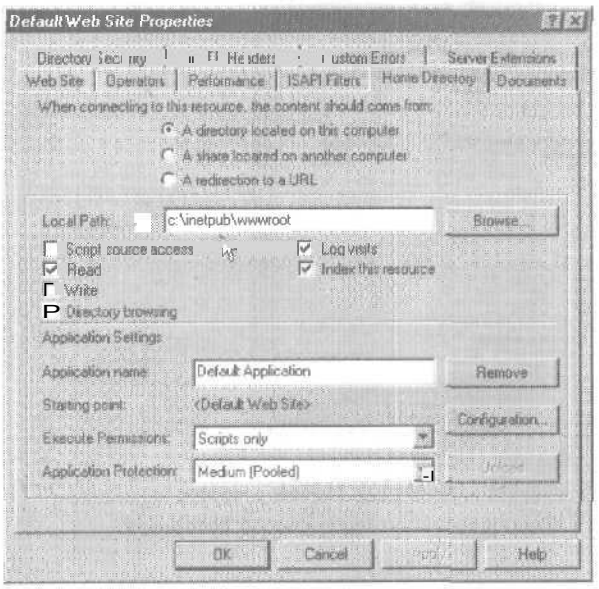


Рис. 14-11. Вкладка Home Directory (Домашний каталог) диалогового окна свойств Web-узла по умолчанию

Создание виртуальных каталогов

Для публикации ресурсов, не входящих в домашний каталог, можно создать виртуальный каталог, который не содержится в домашнем каталоге, однако клиентским браузерам он будет казаться его частью.

Виртуальный каталог имеет псевдоним, применяемый Web-браузерами для обращения к этому каталогу. Пользователям удобнее работать именно с псевдонимом, так как он обычно короче полного пути к каталогу. Кроме того, применение псевдонима безопаснее, потому что пользователи не будут знать физического местоположения Ваших файлов на сервере и не смогут их изменить. Кроме того, при перемещении каталога Вам не придется менять его адрес URL — достаточно поставить в соответствие псевдониму новое местоположение каталога.

Для простого Web-узла нет нужды создавать виртуальные каталоги. Можно просто поместить все файлы в домашний каталог узла. Если же нужно построить сложный Web-узел или задать различным его частям разные адреса URL, можно создать виртуальные каталоги.

Чтобы создать виртуальный каталог, запустите оснастку Internet Information Services и выберите требуемый Web- или FTP-узел, в меню Action (Действие) — New (Создать), а затем — команду Virtual Directory (Виртуальный каталог) (рис. 14-12).

В диспетчере Internet Services Manager (HTML) для публикации информации в виртуальный каталог используется та же ссылка, что и для создания нового узла. Выбрав в Internet Services Manager (HTML) нужный узел, на левой панели щелкните ссылку New (Создать) — запустится мастер IIS New Site (Мастер создания узлов 11S). Перейдя в следующее окно мастера, щелкните переключатель Virtual Directory (Виртуальный каталог) для публикации в новый виртуальный каталог.

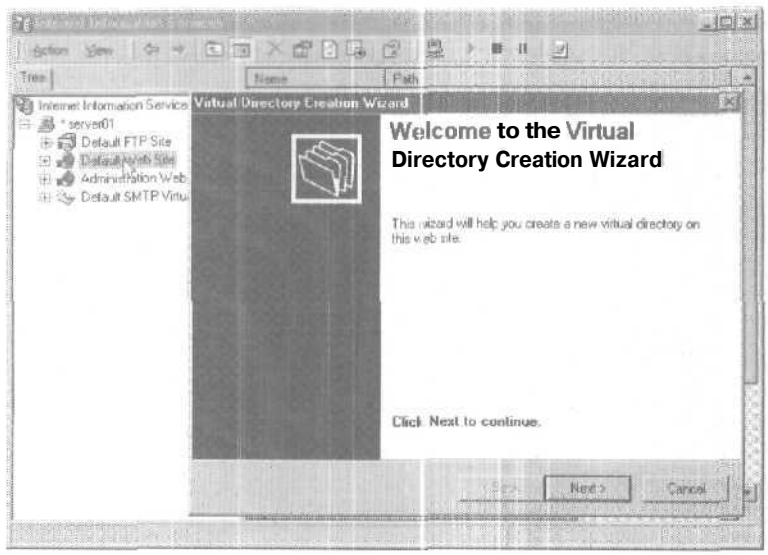


Рис. 14-12. Создание виртуального каталога для Web-узла Default с помощью мастера Virtual Directory Creation (Мастер создания виртуальных каталогов)

Переадресация запросов

Когда браузер запрашивает страницу, находящуюся на Вашем Web-узле, Web-сервер ищет ее по заданному URL, после чего возвращает ее браузеру. При перемещении страницы не всегда удается исправить все ссылки на нее, заменив в них старый URL страницы на новый. Для решения этой проблемы можно настроить Web-сервер так, чтобы он предоставлял браузеру новый URL страницы. При этом, не обнаружив страницу по старому URL, браузер повторно запросит ее, используя новый URL. Этот процесс называется *переадресацией запроса браузера* (redirecting a browser request), или *переадресация на другой URL* (redirecting to another URL). Переадресация запроса к странице происходит по тому же принципу, что и использование пересылочного адреса при доставке почты. Наличие пересылочного адреса гарантирует, что все письма и посылки, отправленные по предыдущему адресу Вашего проживания, будут затем доставлены на Ваш новый адрес.

Переадресация URL полезна, когда Вы изменяете Web-узел и хотите сделать его часть временно недоступной или когда было изменено имя виртуального каталога и все ссылки на файлы в старом виртуальном каталоге должны указывать на те же файлы в новом виртуальном каталоге.

Для переадресации запросов на Web-узел, виртуальный каталог или другой каталог запустите оснастку Internet Information Services и откройте диалоговое окно свойств соответствующего Web-узла, виртуального каталога или каталога. Перейдите на вкладку Home Directory (Домашний каталог), Virtual Directory или Directory (Каталог), шелкните переключатель A Redirection To A URL (Постоянный адрес URL) и введите новый URL в поле Redirect To (Адрес).

Другие инструменты

Часто после того, как содержание Web-узла было затребовано, возникает необходимость его динамического изменения перед передачей браузеру. IIS реализует эту функцию с помощью *включений на стороне сервера* (server-side includes, SSI) и среды разработки сценариев ASP.

SSI обеспечивают выполнение многих задач по управлению Web-узлом — от динамического добавления текущего времени до выполнения специальной команды оболочки при каждом запросе файла. Команды SSI — *директивы* (directives) — добавляются к Web-страницам во время их разработки. При запросе страницы Web-сервер анализирует синтаксис директив на странице, а затем выполняет их. Наиболее часто используемые директивы SSI осуществляют вставку или включение содержимого файлов в Web-страницы. Так, если нужно постоянно обновлять рекламу на Web-странице, можно использовать SSI, чтобы включить HTML-страницу с рекламой в Web-страницу. Чтобы изменить рекламу, измените только HTML-страницу, содержащую ее текст. Для использования SSI не нужно знать язык создания сценариев — хватит знакомства с синтаксисом директив.

ASP — это серверная среда создания сценариев, позволяющая динамически изменять содержание Web-страниц. Хотя главное предназначение — разработка Web-приложений, ASP предоставляет возможности, облегчающие управление Web-узлами. Например, ASP позволяет отслеживать посетителей Web-узла, или настроить содержание Web-узла под браузер. Однако, в отличие от SSI, ASP требует использования языка сценариев, например VBScript или JScript.

Управление содержанием Web-узла с помощью ASP

В Windows 2000 входит Microsoft ASP — серверная среда создания сценариев, которую можно использовать для автоматизации и централизации выполнения многих задач по управлению Web-узлом.

Сценарии

Сценарий (script) — это набор команд и инструкций, позволяющий изменять содержание Web-страниц программно. Если Вы когда-либо посещали Интернет-магазины, то встречались со сценариями.

Сценарии бывают клиентскими и серверными. Первые выполняются на Web-браузере. Они встраиваются в Web-страницу между тэгами HTML <SCRIPT> и </SCRIPT>. Если Вы просмотрите какую-нибудь динамичную Web-страницу в виде HTML, то обнаружите в ней клиентский сценарий. Вторые выполняются на Web-сервере и используются в основном для изменения Web-страниц перед отправкой их на браузер. Эти сценарии позволяют обработать вводимые пользователем данные или определить количество посещений Web-узла. Серверный сценарий осуществляет «сборку» Web-страницы перед отправкой обозревателю. Это облегчает управление содержанием Web-узла.

Обзор ASP

Серверные сценарии позволяют автоматизировать задачи управления Web-узлами так же, как автоматизировать стандартные задачи в электронных таблицах или текстовых редакторах помогают макросы. Допустим Вам нужно изменить Web-узел, состоящий из нескольких десятков страниц, каждая из которых содержит информацию в стандартном формате (например логотип компании, данные об авторском праве и др.). Если выполнять эту работу вручную, она займет много времени. Лучше автоматизировать ее при помощи ASP.

ASP — это мощная серверная среда, позволяющая создавать сценарии, применяя такие средства, как Notepad. Используя ASP, можно, например, создать центральный файл, содержащий общую для всех страниц Web-узла информацию. Затем при разработке Web-узла в каждую страницу можно добавить состоящий из одной строки сценарий, вставляющий в эту страницу содержимое центрального файла. В этом случае для изменения, допустим, навигационного меню Вашего узла достаточно изменить центральный файл. Эти изменения станут автоматически видны пользователю после перезагрузки содержимого Web-узла.

Для отделения команд сценариев от обычного текста и HTML в ASP используются *разделители* (delimiters). В отличие от разделителей < и >, используемых в HTML для обозначения тегов, обрабатываемых обозревателем Web, для выделения команд сценариев, выполняющихся на сервере, применяются разделители <% и %>.

Следующий пример иллюстрирует работу ASP:

```
<%
author = "Max"
department = "Quality Assurance"
%>

This page was updated <B>today</B>, by <%= author %> from
the <%= department %> Department.
```

Просматривая страницу, содержащую этот сценарий, из Web-браузера, пользователь увидит текст:

This page was updated **today,** by Max from the Quality Assurance Department.

Однако при просмотре исходного текста Web-страницы через Web-браузер можно увидеть только следующий текст и HTML:

```
This page was updated <B>today</B>, by Max from the Quality Assurance
Department.
```

Дело в том, что сценарий (т. е. команды между разделителями <% и %>) выполняется на сервере, а на пользовательский обозреватель возвращается только готовый HTML-код.

Все ASP-файлы должны как минимум иметь расширение .asp и содержать команды языка сценариев, например Microsoft Visual Basic Scripting Edition (VBScript) или Microsoft JScript. Об основах создания сценариев Вы узнаете на Web-узле Microsoft Windows Script Technologies по адресу *http://msdn.microsoft.com/scripting/*.

Упражнение 1: изучение Web-узла Administration

Вы настроите Web-узел Administration с помощью оснастки Internet Information Services. Вы сконфигурируете права доступа к этой секретной части Web-сервера. Затем с помощью диспетчера Internet Service Manager (HTML) Вы проверите возможность доступа к узлу. Выполняйте упражнение на Server01.

► Задание 1: настройте Web-узел Administration с помощью оснастки Internet Information Services

Вы используете оснастку Internet Information Services для настройки Web-узла Administration.

1. Зарегистрируйтесь на ServerOl как Administrator (Администратор) с паролем **password.**
2. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Internet Services Manager (Диспетчер служб Интернета).

   Откроется окно оснастки Internet Information Services.
3. В дереве консоли раскройте узел * server01.

   Под * serverO! Вы увидите контейнеры Default FTP site (FTP-узел по умолчанию), Default Web site (Веб-узел по умолчанию), Administration Web site (Администрирование веб-узла) и Default SMTP Virtual Server (Виртуальный SMTP-сервер по умолчанию).
4. В дереве консоли раскройте узел Administration Web site (Администрирование веб-узла), Вы увидите два виртуальных каталога: IISAdmin и IISHelp.

5. В дереве консоли щелкните папку Administration Web site.
6. В меню Action (Действие) выберите команду Properties (Свойства).

   Откроется диалоговое окно Administration Web Site Properties (Свойства: Администрирование веб-узла).
7. Запомните номер порта TCP, содержащийся в поле TCP Port (TCP-порт) на вкладке Web Site (Веб-узел).

   Этот номер (случайное число от 2000 до 9999) будет обозначен здесь как *tcp-порт*.
8. Убедившись, что в списке под флажком Enable Logging (Вести журнал) выбран пункт W3C Extended Log File Format (Расширенный формат файла журнала W3C), щелкните кнопку Properties (Свойства).

   Откроется диалоговое окно Extended Logging Properties (Расширенные свойства ведения журнала). Заметьте: файл журнала хранится в папке %WinDir%\System32\LogFiles, т. е. в папке %SystemRoot%\System32\LogFiles.
9. Перейдите на вкладку Extended Properties (Расширенные свойства).
10. Прокрутите список параметров и пометьте флажок Process Accounting (Учет процессов).
11. Щелкните кнопку OK, чтобы закрыть диалоговое окно Extended Logging Properties (Расширенные свойства ведения журнала).
12. В окне свойств Web-узла перейдите на вкладку Directory Security (Безопасность каталога).
13. В группе Anonymous Access And Authentication Control (Анонимный доступ и проверка подлинности) щелкните кнопку Edit (Изменить).

    Откроется диалоговое окно Authentication Methods (Способы проверки подлинности). Обратите внимание, что для Web-узла Administration по умолчанию не доступны ни анонимный доступ, ни обычная аутентификация — только интегрированная аутентификация Windows.

    Это значит, что клиентский браузер, устанавливающий соединение с Web-узлом Administration, должен поддерживать аутентификацию NTLM либо аутентификацию Kerberos. Тип интегрированной аутентификации Windows зависит от браузера.
14. Пометьте флажок Digest Authentication For Windows Domain Servers (Краткая проверка для серверов доменов Windows).

    Появится сообщение, что для доступа к узлу можно использовать только учетные записи домена Windows 2000 и что пароли будут храниться в виде обычного зашифрованного текста.
15. Щелкните кнопку Yes (Да).
16. Щелкните кнопку OK, чтобы закрыть диалоговое окно Authentication Methods.
17. В окне Administration Web Site Properties в группе IP Address And Domain Name Restrictions (Ограничения IP-адресов и имен доменов) щелкните кнопку Edit (Изменить).

    Откроется диалоговое окно IP Address and Domain Name Restrictions (Ограничения IP-адресов и имен доменов). Заметьте, что выбран переключатель Denied Access (Запрещен доступ) и что доступ разрешен только локальному адресу возвратной петли — 127.0.0.1.
18. Щелкните переключатель Granted Access (Разрешен доступ), чтобы открыть доступ к Web-узлу Administration со всех компьютеров Вашей учебной сети.

    Дополнительно можно указать IP-адреса, диапазон IP-адресов или компьютеры внутри определенного домена, которым разрешен доступ к Web-узлу Administration. Последний вариант требует значительных затрат ресурсов, и поэтому для большинства реализаций IIS 5.0 использовать его не рекомендуется.

19. Щелкните кнопку OK
20. Щелкните кнопку OK, чтобы закрыть окно Administration Web Site Properties,

    Откроется диалоговое окно Inheritance Overrides (Изменение наследования), сообщающее, что дочерние узлы также определили значение свойства Authentication Methods (Способы проверки подлинности), перезаписав только что заданное Вами значение.
21. В списке Child Nodes (Дочерние узлы) щелкните IISAdmin, а затем — кнопку OK.

    Снова откроется диалоговое окно Inheritance Overrides (Изменение наследования) для дочернего узла IISHelp.
22. Щелкните в списке IlSHelp, а затем — кнопку OK.
23. Закройте оснастку Internet Information Services.

► Задание 2: обратитесь к Web-узлу Administration из диспетчера Internet Service Manager (HTML)

Установите соединение с Web-узлом Administration, параметры которого Вы только что изменили.

Примечание Значение переменной *tcp-порт* следует заменить на значение порта TCP, которое Вы запомнили при настройке Web-узла.

1. На Server01 в меню Start (Пуск) выберите команду Run (Выполнить).

   Откроется диалоговое окно Run (Запуск программы).
2. В поле Open (Открыть) введите **http://server01:<tcp-порт>** и щелкните кнопку OK.

   Запустится Internet Explorer, сообщая, что для администрирования через обозреватель Web применяется небезопасное соединение.

   Это значит, что хотя сведения об аутентификации, передаваемые по сети между обозревателем и Web-узлом Administration, защищены, информация, передаваемая после установления соединения, может быть перехвачена.
3. В окне Internet Explorer вы увидите интерфейс диспетчера Internet Services Manager (HTML).
4. При помощи ссылок на левой панели исследуйте Web-узлы, представленные в главном окне интерфейса.
5. Закройте Internet Explorer.

► Задание 3: настройте доступ к Web-узлу Administration с помощью протокола SSL

Установите безопасное соединение с Web-узлом Administration при помощи протокола SSL. Для этого выпустите свой сертификат сервера с помощью ServerOI и служб Certificate Services.

Примечание Службы Certificate Services были установлены в занятии 1, главы 11.

1. На ServerOI вызовите оснастку Internet Information Services.
2. В дереве консоли раскройте узел * server01.
3. Щелкните папку Administration Web site.
4. В меню Action (Действие) выберите команду Properties (Свойства).

   Откроется диалоговое окно Administration Web Site Properties.
5. Перейдите на вкладку Directory Security (Безопасность каталога).
6. В группе Secure communications (Безопасные подключения) щелкните кнопку Server Certificate(Сертификат).

Откроется окно мастера сертификатов IIS.

7. Щелкните кнопку Next (Далее).
8. Убедившись, что выбран переключатель Create A New Certificate (Создание нового сертификата), щелкните кнопку Next (Далее).

   Откроется окно Delayed or Immediate Request (Отложенный или немедленный запрос).
9. Щелкните переключатель Send The Request Immediately To An Online Certification Authority (Немедленно отправить запрос в локальную службу сертификации), а затем — кнопку Next (Далее).

   Откроется окно Name and Security Settings (Настройка имени и безопасности).

   Заметьте, что сертификату по умолчанию присвоено имя Administration Web site (Администрирование веб-узла) и его длина составляет 512 бит.
10. Щелкните кнопку Next (Далее).

    Откроется окно Organization Information (Сведения об организации).
11. В списке Organization (Организация) введите **Microsoft Corporation,** а в списке Organizational Unit (Подразделение) — **Microsoft Press.**
12. Щелкните кнопку Next (Далее).

    Откроется окно Your Site's Common Name (Полное имя узла).
13. В поле Common Name (Полное имя) введите **server01.microsoft.com** и щелкните кнопку Next (Далее).

    Откроется окно Geographical Information (Сведения о местоположении).
14. В списке State/Province (Область край республика) введите **Washington**, а в списке City/Locality (Город) — Redmond.
15. Щелкните кнопку Next (Далее).

    Откроется окно Choose a Certification Authority (Выбор службы сертификации). В списке центров сертификации вы увидите server01.microsoft.com\Enterprise CA.
16. Щелкните кнопку Next (Далее).

    Откроется окно Certificate Request Submission (Отправка запроса сертификата).
17. Изучите сводку параметров и щелкните кнопку Next (Далее).

    Через некоторое время откроется окно Completing the Web Server Certificate (Завершение работы мастера сертификатов веб-сервера).
18. Щелкните кнопку Finish (Готово).

    Откроется диалоговое окно Administration Web Site Properties. Кнопки View Certificate (Просмотр) и Edit (Изменить) в группе Secure communications (Безопасные подключения) этого окна стали доступными.
19. В группе Secure communications (Безопасные подключения) этого окна шелкните кнопку Edit (Изменить).

    Откроется диалоговое окно Secure Communications (Безопасные подключения).
20. Пометьте флажок Require Secure Channel (SSL) (Требуется безопасный канал).
21. Убедитесь, что выбран переключатель Ignore Client Certificates (Игнорировать сертификаты клиентов) и щелкните кнопку OK.

    Откроется диалоговое окно Administration Web Site Properties.
22. Перейдите на вкладку Web Site (Веб-узел).
23. В поле SSL Port (Порт SSL) наберите 5000.
24. Щелкните кнопку OK.
25. Закройте оснастку Internet Information Services.

▶ **Задание 4:** проверьте **доступ к защищенному Web-узлу Administration**

Проверьте доступ к Web-узлу Administration после конфигурирования SSL.

1. На Server01 в меню Start выберите команду Run.

   Откроется диалоговое окно Run (Запуск программы).

2. В поле Open (Открыть) введите **http://server01:<*tcp-порт*>** и щелкните OK.

   Значение переменной tcp-порт возьмите из первой процедуры упражнения.

   Запустится Internet Explorer, сообщая, что эту страницу следует просматривать через безопасный канал.

3. В Internet Explorer в поле адреса введите **https://server01.microsoft.com:5000**. 5000 — это значение *SSL-порт,* которое Вы ввели на вкладке Web Site (Веб-узел).

   Появится сообщение, что Вы будете просматривать информацию через безопасное соединение.

4. Щелкните кнопку OK.

   Откроется диалоговое окно Enter Network Password (Ввод сетевого пароля).

5. В поле User Name (Имя пользователя) введите **Administrator** (Администратор), в поле Password (Пароль) — **password,** в поле Domain (Домен) — **microsoft.**

6. Пометьте флажок Save This Password In Your Password List (Сохранить пароль в списке паролей) и щелкните кнопку OK.

   Вы увидите интерфейс диспетчера служб Интернета. В правом нижнем углу строки состояния появился значок замка.

7. Установите указатель мыши на этом значке.

   Появится подсказка SSL secured (56 Bit) [SSL-защита (56 бит)]. В диалоговом окне свойств узла можно задать 128-разрядное шифрование. Хотя ранее Вы указали, что при соединении необходимо использовать протокол SSL, Вы не потребовали 128-разрядного шифрования.

8. Дважды щелкните значок замка.

   Откроется диалоговое окно Certificate (Сертификат).

9. Просмотрите информацию в этом окне.

   Из диалогового окна Certificate (Сертификат) можно запустить мастер Certificate Import (Мастер импорта сертификатов), чтобы скопировать информацию о сертификате с локального компьютера в хранилище сертификатов.

10. Щелкните кнопку OK.

11. Закройте диспетчер служб Интернета.

Резюме

По сравнению с предыдущими версиями I1S 5.0 обладает большей надежностью, производительностью и управляемостью, улучшенной системой безопасности и средой разработки приложений. В IIS 5.0 появился ряд новых возможностей (например поддержка пула внепроцессных приложений), позволяющих повысить надежность и производительность Web-узлов. IIS 5.0 облегчает управление Web-сервером. Например, установка IIS 5.0 интегрирована в процесс установки Windows 2000 Server. Для упрощения настройки безопасности в IIS 5.0 появились три новых мастера. Система безопасности в IIS 5.0 использует преимущества стандартов безопасности Интернета, поддерживаемых Windows 2000. В IIS 5.0 легче отлаживать и развертывать Web-приложения. Установку и удаление IIS можно осуществить одним из трех способов: установив или обновив Windows 2000, используя утилиту Add/Remove Programs в Control Panel или файл ответов unattended.txt при автоматической установке. Во время установки IIS 5.0 создаются Web-узлы Default и Administration, FTP-узел Default и сервер Default SMTP Virtual Server. Для создания Web-узла надо указать папки, где будут храниться публикуемые документы. Каждый Web- и FTP-узел должен иметь свой домашний каталог. Для публикации ресурсов, не входящих в него, можно создать виртуальный каталог. В Windows 2000 входит Microsoft ASP — серверная среда создания сценариев, которую можно использовать для автоматизации и централизации выполнения многих задач по управлению Web-узлом.

Занятие 2. Управление средой Web

При установке IIS создается Web-узел Default, предоставляя в Ваше распоряжение готовую среду Web. Вы можете изменять эту среду, подстраивая ее под свои потребности. Кроме того, Вы можете использовать WebDAV, позволяющую совместно работать с документами в Интернете или интрасети. Мы рассмотрим управление Web- и FTP-узлами и публикацию с помощью WebDAV. Так как принципы управления Web- и FTP-узлами одни и те же, они будут обсуждаться вместе.

Изучив материал этого занятия, вы сможете:

- ✓ администрировать Web- и FTP-узлы;
- ✓ управлять публикацией с помощью WebDAV.

Продолжительность занятия - около 35 минут.

Администрирование Web- и FTP-узлов

Первоначально каждое доменное имя, например www.microsoft.com, однозначно идентифицировало индивидуальный компьютер. Однако в IIS 5.0 на одном компьютере с Windows 2000 Server может одновременно быть размещено несколько Web- и FTP-узлов. Каждый Web-узел может иметь одно или несколько доменных имен. Так как узлы продолжают ассоциироваться с индивидуальными компьютерами, их иногда называют *виртуальными серверами* (virtual servers).

Web- и FTP-узлы

В Интернете или интрасети Вы можете создавать несколько Web- и FTP-узлов на компьютере с Windows 2000 Server. Это можно сделать:

- добавив к IP-адресу номера портов;
- присвоив каждому сетевому адаптеру свой IP-адрес;
- присвоив одному сетевому адаптеру несколько доменных имен и IP-адресов, используя имена заголовков хостов.

На рис. 14-13 системный администратор установил на сервер организации в интрасети Windows 2000 Server с IIS, в результате чего по умолчанию был создан узел *http://CompanyServer*. Затем администратор создает еще два Web-узла — для отдела маркетинга и отдела кадров.

CompanyServer, Marketing и HumanResources кажутся пользователям самостоятельными Web-узлами, хотя и располагаются на одном компьютере. Так как каждый узел допускает независимое от других узлов конфигурирование параметров доступа и административных разрешений, его система безопасности ничем не отличается от системы безопасности узла, размещаемого на отдельном компьютере.

Примечание При размещении большого количества узлов на одном компьютере нужно учитывать требования к аппаратным средствам.

Свойства и наследование свойств узлов

Свойства — это значения, которые могут быть заданы Web-узлу. Например, используя оснастку Internet Information Services, можно поменять номер порта TCP для Web-узла Default с 80 (установленного по умолчанию) на другое значение. Свойства узла отображаются в его диалоговом окне свойств (рис. 14-14) и хранятся в БД, называемой метабазой.

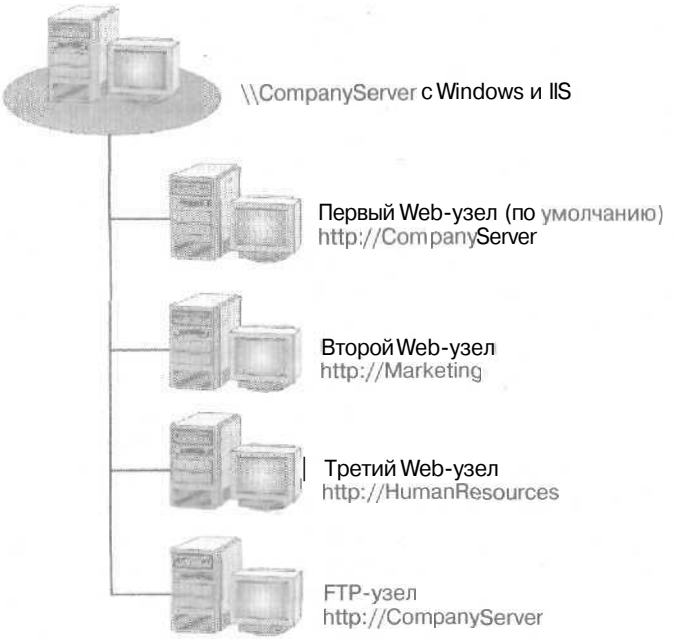


Рис. 14-13. Интрасеть с несколькими Web-узлами

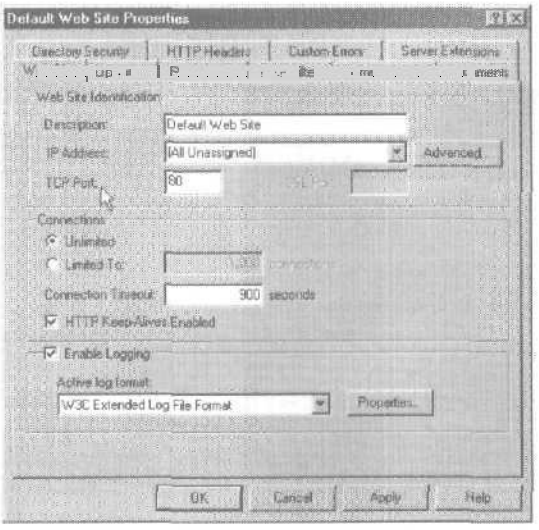


Рис. 14-14. Диалоговое окно свойств Web-узла Default

При установке IIS свойствам присваиваются значения по умолчанию. **Вы** можете либо оставить их в силе, либо изменить. Умелая настройка свойств позволяет повысить производительность и увеличить безопасность.

Примечание В упражнении 1 этой главы Вы уже настраивали свойства Web-узла Administration, чтобы повысить безопасность этой важной части IIS.

Свойства могут быть заданы на уровне узлов, каталогов и файлов. Свойства нижнего уровня (например уровня каталога) наследуют свойства верхнего уровня (например уровня узла). Свойства нижнего уровня можно задать индивидуально. (При этом значения этих свойств не будут переопределены в случае изменения свойств более высокого уровня. Вместо этого появится запрос: хотите ли Вы изменить значения индивидуальных параметров узла, каталога или файла, чтобы они соответствовали новым значениям по умолчанию верхнего уровня.)

Значения некоторых свойств представляют собой список. Например, в качестве документа, загружаемого по умолчанию (т. е. когда пользователь не указал имя файла в URL), можно указать список документов. Другие примеры таких свойств — нестандартные сообщения об ошибках, список доступа TCP/IP, привязки сценариев и MIME. Хотя список состоит из нескольких значений, он рассматривается IIS как единое целое. При редактировании списка на уровне каталога и последующем изменении его на уровне узла список на уровне каталога полностью заменяется новым — списки не объединяются. Значения свойств-списков отображаются только для свойств верхнего уровня (или свойств уровня узла или каталога, для которых значения по умолчанию были изменены). Если свойство-список наследует свое значение по умолчанию, то это значение не отображается.

Чтобы просмотреть основные свойства, серверные расширения, параметры пропускной способности и привязки MIME, в оснастке Internet Information Services выберите узел компьютера и откройте его окно свойств. Для этого можно также использовать диспетчер Internet Services Manager (HTML). На рис. 14-15 изображено окно свойств верхнего уровня для службы WWW,

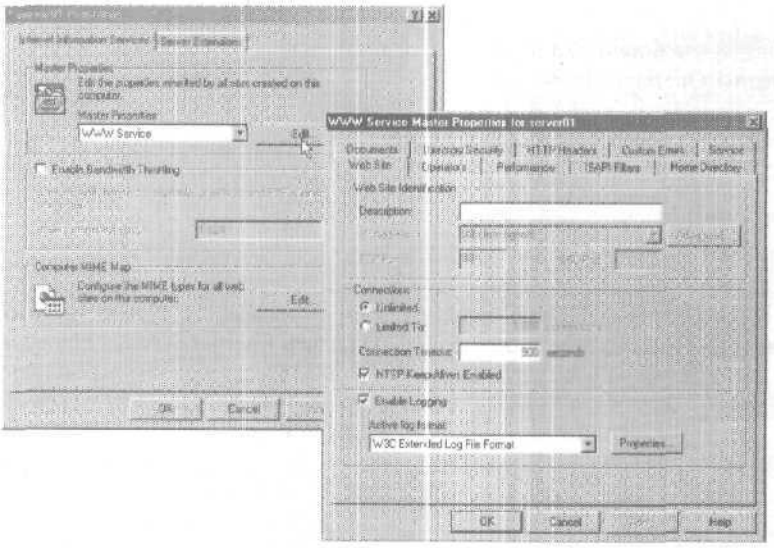


Рис. 14-15. Диалоговое окно WWW Service Master Properties for Server01 (Основные свойства WWW-службы для ServerOl)

В интерфейсе Internet Services Manager (HTML) для просмотра свойств верхнего уровня надо щелкнуть ссылку Master Properties (Основные свойства) (рис. 14-2).

Хотя фильтры Internet Server API (ISAPI) отображаются в виде списка, они таковыми не являются. Фильтры, созданные на уровне узла, добавляются к списку фильтров верхнего уровня. Если два фильтра имеют одинаковые установки приоритета, то сначала загружается фильтр верхнего уровня, а затем — фильтр уровня узла. Установленные фильт-

ры ISAPI и их приоритеты можно просмотреть на вкладке ISAPI Filters (Фильтры ISAPI) окна WWW Service Master Properties (Основные свойства WWW-службы) или в окне свойств любого Web-узла.

Если установленные по умолчанию значения свойств были изменены, то создаваемые впоследствии Web- и FTP-узлы их унаследуют.

Группа Operators

Operators (Операторы) представляет собой группу пользователей, имеющих ограниченные административные привилегии для отдельных Web-узлов. Члены этой группы могут управлять параметрами, относящимися только к узлам, находящимся в их компетенции. У них нет доступа к параметрам, определяющим работу IIS в целом, компьютера-сервера с Windows, на котором установлен IIS, или сети.

Например, поставщик услуг Интернета, размещающий узлы большого числа различных организаций, может назначить представителей каждой организации операторами соответствующего Web-узла. Этот метод распределенного администрирования сервера имеет следующие преимущества.

- Каждый член группы Operators может действовать как администратор узла, изменяя при необходимости его наполнение и параметры. Например, оператор может устанавливать разрешения доступа к Web-узлу, включать/отключать ведение журнала, изменять документ по умолчанию или заголовок, устанавливать временные параметры хранения содержимого.
- Оператор Web-узла не имеет права изменять идентификационные параметры узлов, задавать имя или пароль анонимного пользователя, настраивать ширину полосы пропускания, создавать виртуальные каталоги или изменять их расположение, а также изменять существующую изоляцию приложений.
- Так как члены группы Operators имеют более ограниченные привилегии, чем администраторы Web-узла, они не могут удаленно просматривать файловую систему, что лишает их возможности управлять свойствами файлов и каталогов (если не используется путь UNC).

Удаленное администрирование узлов

Так как выполнять административные задачи на компьютере с IIS не всегда удобно, были разработаны два инструмента удаленного администрирования. Для изменения свойств узла с компьютера, подключающегося к серверу через Интернет или прокси-сервер, можно использовать основанный на интерфейсе обозревателя диспетчер Internet Services Manager (HTML). При работе в интрасети можно использовать как упоминавшийся выше диспетчер, так и оснастку Internet Information Services. Хотя диспетчер Internet Services Manager (HTML) обладает практически теми же возможностями, что и оснастка, с его помощью нельзя изменить свойства, требующие координации с утилитами Windows (например привязку сертификата).

Примечание В предыдущих версиях оснастка Internet Information Services называлась Internet Services Manager (Диспетчер служб Интернтеа). Это название до сих пор используется в программной группе Administrative Tools (Администрирование).

Для управления свойствами IIS в диспетчере Internet Services Manager (HTML) используется узел, который в списке узлов отображается как Administration Web site (Администрирование веб-узла). При установке IIS этому узлу присваивается номер порта, выбираемый случайным образом между 2000 и 9999. Этот узел отвечает на запросы браузера, направленные к любому доменному имени, связанному с этим компьютером (при условии,

что кроме имени узла указывается еще и номер порта). Если используется базовая аутентификация, то при соединении с узлом администратора попросят ввести имя пользователя и пароль. Право доступа к Web-узлу Administration имеют только члены трупп Administrators и Operators.

Примечание Хотя HTML-версия диспетчера служб Интернета реализует большинство функций оснастки Internet Information Services, она ограничена возможностями отображения Web-страниц. Поэтому в ней не поддерживается вызов контекстного меню щелчком правой кнопкой объекта интерфейса, а многие из знакомых кнопок на панели инструментов и заголовков вкладок отображаются как ссылки на левой панели окна браузера. Вследствие этих различий инструкции в документации могут не всегда точно совпадать с действиями, выполняемыми в HTML-диспетчере.

Для удаленного администрирования IIS через сетевое соединение можно использовать службы Terminal Services. При этом на удаленном компьютере не требуется устанавливать MMC или оснастку Internet Information Services.

При удаленном администрировании IIS 5.0 можно пользоваться электронной документацией. Для доступа к ней откройте Web-узел Administration и щелкните значок книги в правом верхнем углу домашней страницы. Откроется новое окно, имеющее URL *http://<имя_сервера>/iishelp/iis/misc/default.asp*, где *имя_сервера* — идентификатор компьютера (IP-адрес, имя компьютера или полное доменное имя), на котором установлен IIS.

Поиск в электронной документации по IIS основан на использовании службы Indexing Service (Служба индексирования). По умолчанию она устанавливается вместе с Windows 2000 Server и конфигурируется для ручного запуска. Настройка службы Indexing Service осуществляется из оснастки Computer Management — раскройте узел Services and Applications (Службы и приложения). Так как документация по IIS 5.0 проиндексирована для поиска, добавьте в папку Web службы Indexing Service полный физический путь к папке iisHelp. Сконфигурировав службу Indexing Service, настройте ее автоматический запуск из оснастки Services (Службы).

Примечание Службе индексирования требуется много ресурсов, особенно если нужно проиндексировать большой объем материала. Поэтому для выполнения этой функции следует выделить компьютер достаточной мощности.

Перезапуск FTP

Применяется при потере сетевого соединения во время загрузки файлов. Клиентам, поддерживающим дозагрузку по протоколу FTP, нужно лишь восстановить FTP-соединение, и передача файла автоматически возобновится с того места, где была прервана.

Примечание В IIS 5.0 дозагрузка по протоколу FTP невозможна при использовании FTP для запроса на получение файла по маске (MGET), при передаче файлов на сервер (PUT) и при загрузке файлов размером более 4 Гб.

Управление узлами

Управление узлами включает в себя ряд задач, наиболее важные из которых — запуск, остановка и создание узлов, задание имени узла и перезапуск IIS.

Запуск и завершение работы узлов

По умолчанию узлы запускаются автоматически при перезапуске компьютера. При завершении работы узла работа служб Интернет также завершается, и они выгружаются из памяти компьютера. При приостановке работы узла службы Интернет прекращают устанавливать новые соединения, однако уже поступившие запросы продолжают обрабатываться. При запуске узла происходит запуск или возобновление работы служб Интернет.

Для запуска, завершения и приостановки работы узла используется оснастка Internet Information Services. Выбрав в ней нужный узел, щелкните кнопку Start Item (Запуск объекта), Stop Item (Остановка объекта) или Pause Item (Пауза объекта) на панели инструментов.

Примечание При незапланированном завершении работы узла оснастка Internet Information Services может некорректно отображать состояние сервера. Поэтому сначала щелкните кнопку Stop, и только затем выполните перезапуск, щелкнув кнопку Start.

Создание узлов

Чтобы создать новый узел, из оснастки Internet Information Services запустите мастер Web Site Creation (Мастер создания веб-узлов), **FTP** Site Creation (Мастер создания FTP-узла) или SMTP Virtual Server (Мастер создания виртуального SMTP-сервера) в зависимости от того, какой узел Вы хотите создать. Для этого выберите компьютер или узел, в меню Action (Действие) — New (Создать), а затем — команду Web Site (Узел Web), FTP Site (Узел FTP) или SMTP Virtual Server (Виртуальный SMTP-сервер).

Примечание Мастер SMTP Virtual Server далее не рассматривается.

Следуя указаниям, появляющимся на экране, введите идентификационную информацию о новом узле. Укажите адрес порта, домашний каталог и имя заголовка узла (если несколько узлов имеют один и тот же IP-адрес).

Примечание Элемент All Unassigned (Значения не присвоены) списка Enter the IP address to use for this Web Site (Введите IP-адрес для веб-узла) мастера создания Web-узла [или списка IP Address (IP-адрес) мастера создания FTP-узла] обозначает те IP-адреса, которые были присвоены компьютеру, но не были назначены конкретному узлу. Все эти адреса применяются для обращения к Web-узлу Default. Использовать неназначенные адреса может только один узел.

Задание имени для Web-узла

Каждый Web-узел (виртуальный сервер) имеет имя. Кроме того, он может иметь одно или несколько имен заголовков хостов, используемых при размещении нескольких узлов на одном компьютере. Имена заголовков хостов поддерживаются не всеми обозревателями. Этой возможностью не обладают, например, обозреватели Internet Explorer до версии 3.0 и Netscape Navigator до версии 2.0.

Если обозреватель, не поддерживающий имена заголовков хостов, попытается соединиться с Вашим узлом, он будет направлен на Web-узел Default, имеющий тот же IP-адрес (если этот узел доступен). Естественно, Web-узел Default может быть вовсе не тем узлом, с которым пользователь хотел соединиться. Если обозреватель запрашивает узел, который в это время остановлен, он также будет направлен на Web-узел Default. Поэтому подумайте о том, какую информацию должен содержать Web-узел Default. Например, поставщик услуг Интернета обычно по умолчанию отображает свою домашнюю страницу, а не узел одного из своих клиентов. В результате пользователи, обращающиеся к остановленному

узлу, не попадут случайно на чужой узел. Кроме того, в узел Default можно встроить сценарий, поддерживающий имена заголовков хостов для ранних версий браузеров.

Чтобы задать узлу имя, в оснастке Internet Information Services выберите нужный Web-узел и откройте его диалоговое окно свойств, перейдите на вкладку Web Site (Веб-узел) и введите его имя в поле Description (Описание) (рис. 14-14).

Запуск, остановка, перезапуск и перезагрузка IIS

Используя оснастку Internet Information Services в IIS 5.0, можно остановить, запустить, перезагрузить все службы Интернета и перезагрузить сервер. Функции остановки, запуска и перезапуска уменьшают вероятность того, что при неправильной работе или зависании приложений Вам придется перезагружать сервер.

Функция перезапуска обеспечивает удобный механизм остановки и последующего запуска служб Интернета. Для перезапуска IIS в дереве консоли выберите узел компьютера и в меню Action (Действие) выберите команду Restart IIS (Перезапуск IIS). На рис. 14-16 показано открывающееся в результате этого окно Stop/Start/Reboot (Остановка/запуск/перезагрузка).

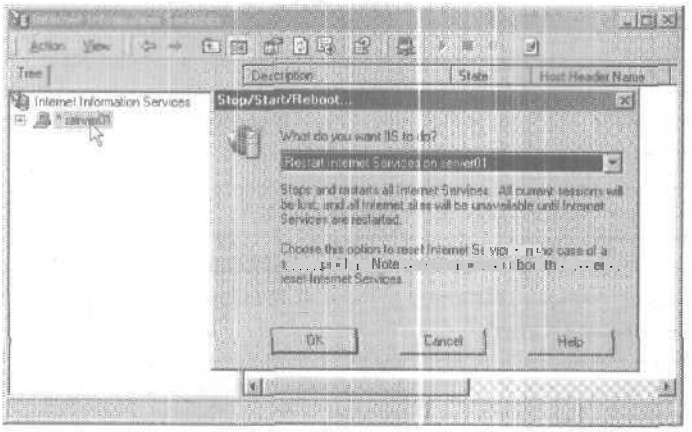


Рис. 14-16. Перезапуск служб Интернета на Server01

В списке этого окна также содержатся команды запуска и остановки IIS и перезагрузки сервера.

Внимание! При перезапуске служб Интернета остановятся все процессы приложений Drwtsn32.exe, Mtx.exe и Dllhost.exe. Из диспетчера Internet Services Manager (HTML) нельзя остановить или запустить IIS и перезагрузить сервер. Однако как оснастка internet Information Services, так и HTML-интерфейс позволяют запускать, завершать, приостанавливать и возобновлять работу отдельных узлов.

Перезапуск служб Интернета осуществляется из оснастки Internet Information Services. Для этого нельзя использовать оснастку Services из оснастки Computer Management. Так как службы Интернет работают в общем процессе, их остановка и запуск не влияют на работу других служб Windows.

Архивирование и восстановление IIS

Архивирование конфигурации IIS позволяет Вам впоследствии легко к ней вернуться. Действия, которые необходимо выполнить для восстановления конфигурации, зависят от того, были ли службы IIS предварительно удалены и переустановлены.

Чтобы заархивировать конфигурацию IIS, запустите оснастку Internet Information Services. Щелкните в дереве консоли узел компьютера, а в меню Action — команду Backup/Restore Configuration (Архивирование и восстановление конфигурации).

Архивирование позволяет восстанавливать только параметры IIS, но не файлы содержимого. Кроме того, восстановление из архива нельзя произвести после переустановки ОС, а также на других компьютерах с Windows 2000.

Примечание Интерфейс Internet Services Manager (HTML) позволяет архивировать IIS, но для восстановления конфигурации служит оснастка Internet Information Services. Для архивирования IIS из Internet Services Manager (HTML) используется ссылка Backup Configuration (Архивирование конфигурации) на левой панели окна диспетчера (рис. 14-2).

Чтобы восстановить конфигурацию IIS из оснастки Internet Information Services, в дереве консоли щелкните узел компьютера и выберите в меню Action команду Backup/Restore Configuration (Архивирование и восстановление конфигурации). Выбрав нужный архивный файл, щелкните кнопку Restore (Восстановить). На вопрос восстанавливать ли параметры конфигурации, ответьте Yes (Да).

Управление публикацией в WebDAV

WebDAV расширяет возможности протокола HTTP/1.1, позволяя клиентам публиковать, блокировать и управлять ресурсами в Web. Используя WebDAV, интегрированную в IIS, клиенты могут:

- управлять ресурсами в каталоге публикации WebDAV; например, имея соответствующие разрешения, пользователи могут копировать или перемешать файлы в каталоге WebDAV;
- изменять свойства, связанные с определенными ресурсами, например, считывать и изменять информацию о свойствах файла;
- устанавливать и снимать блокировки на ресурсы, в результате читать файл одновременно могут несколько пользователей, а изменять — только один;
- искать файлы в каталоге WebDAV по их содержимому или свойствам.

Настроить каталог публикации WebDAV так же просто, как и виртуальный каталог. После того, как каталог публикации был указан, пользователи с соответствующими разрешениями могут публиковать документы на сервере и управлять файлами в каталоге.

Клиенты WebDAV

Для доступа к каталогу публикации **WebDAV** годится любой клиент, поддерживающий стандартный протокол WebDAV, или один из продуктов Microsoft.

- **Мастер Add Network Place** позволяет Windows 2000 осуществлять соединение с сервером WebDAV и представлять содержимое каталога WebDAV так, как если бы он был частью файловой системы Вашего локального компьютера. Установив соединение, можно перетаскивать файлы, читать и изменять их свойства, а также выполнять другие задачи по управлению файлами.

  Например, если Вы создали каталог WebDAV в Web-узле Default на сервере server01.microsoft.com, обратиться к нему можно по адресу *http://server01.microsoft.com/webdav/*.
- **Internet Explorer** 5 позволяет соединиться с каталогом WebDAV и выполнять те же задачи по управлению файлами, что и Windows 2000.

  Для доступа к виртуальному каталогу посредством Internet Explorer 5 в свойствах виртуального каталога необходимо установить разрешение Directory Browsing.
- Любое приложение **Office 2000** позволяет создавать, публиковать, редактировать и сохранять документы в каталоге WebDAV.

Поиск в WebDAV

Соединившись с каталогом WebDAV, пользователи могут легко и быстро найти файлы по их содержимому или свойствам. Например, можно найти все файлы, содержащие таблицу Word или созданные пользователем Алексей.

Интегрированная безопасность

Будучи интегрированным в Windows 2000 и в IIS 5.0, WebDAV заимствует у них систему безопасности. В частности, он поддерживает разрешения **1IS,** заданные при помоши оснастки Internet Information Services, и *дискретные списки управления доступом (*discretionary access control lists, DACLs) файловой системы NTFS.

Так как клиенты с соответствующими разрешениями могут производить запись в каталог WebDAV, необходим строгий контроль доступа к нему. Для этого в IIS 5.0 имеется интегрированная аутентификация Windows со встроенной поддержкой протокола Kerberos 5, гарантирующая, что правом доступа и записи в каталог WebDAV через интрасеть обладают только уполномоченные пользователи.

Кроме того, в IIS 5.0 имеется краткая аутентификация, предназначенная для серверов доменов Windows и обеспечивающая большую безопасность при использовании паролей и передаче информации через Интернет.

Создание каталога публикации

Чтобы установить каталог публикации, создайте физический каталог в каталоге Inetpub. Например, если Вы хотите назвать каталог публикации WebDAV, путь к нему может быть C:\Inetpub\WebDAV.

На самом деле каталог публикации может быть расположен где угодно, но только не в каталоге Wwwroot (так как задаваемые по умолчанию DACL этого каталога отличаются от других каталогов).

Затем в оснастке Internet Information Services создайте виртуальный каталог для нового Web-узла (в этом случае предварительно создайте Web-узел) или для существующего. В качестве его псевдонима введите **WebDAV** (или другое удобное для Вас имя) и свяжите его с созданным каталогом. Назначьте этому каталогу разрешения доступа Read (Чтение), Write (Запись) и Browsing (Обзор каталогов).

Эти разрешения дают пользователям право публиковать документы и просматривать список файлов в этом виртуальном каталоге. Вы можете предоставить такие же разрешения доступа и ко всему Web-узлу, то есть разрешить клиентам публикацию на всем Web-сервере (хотя по соображениям безопасности делать это не рекомендуется).

Примечание Разрешение Write (Запись) само по себе не дает права клиенту изменять активные страницы сервера (ASP) или другие сценарные файлы. Чтобы разрешить изменение этих файлов, создайте виртуальный каталог, предоставив для него разрешения Write (Запись) и Script source access (Доступ к тексту сценария).

В созданном виртуальном каталоге WebDAV пользователи могут публиковать документы.

Управление безопасностью в WebDAV

Для зашиты сервера используются следующие механизмы: аутентификация клиентов, контроль доступа и отказ в обслуживании.

Аутентификация клиентов

В IIS 5.0 существуют следующие уровни аутентификации.

- **Анонимная.** Право доступа к каталогу имеет любой пользователь, поэтому для каталога WebDAV нельзя использовать этот уровень аутентификации. При отсутствии контроля доступа любой злоумышленник беспрепятственно разрушит Ваш каталог.
- **Обычная.** Пароли посылаются по сети в незащищенном виде и могут быть перехвачены. Поэтому этот уровень можно использовать, только если передаваемые данные шифруются при помощи протокола SSL.
- **Интегрированная Windows.** Аутентификация Integrated Windows — самый эффективный вариант при работе с каталогом WebDAV в интрасети.
- **Краткая.** Самый эффективный способ аутентификации при публикации информации на сервер через Интернет или брандмауэр.

При настройке каталога WebDAV необходимо учитывать, как Вы будете выполнять публикацию. При создании виртуального каталога посредством IIS 5.0 по умолчанию используется как анонимный доступ, так и интегрированная аутентификация Windows. Это приемлемо, когда клиенты соединяются с сервером только для чтения Web-страниц и выполнения сценариев, но не годится для случая, когда клиенты могут публиковать данные в каталог и управлять хранящимися в нем файлами.

Контроль доступа

Для контроля доступа к каталогу WebDAV используются как разрешения IIS 5.0, так и разрешения Windows 2000.

Настройка разрешений Web

Настраивая разрешения Web, надо учитывать назначение публикаций.

- **Разрешения Read (Чтение), Write (Запись), Directory** Browsing **(Обзор** каталога). Позволяют клиентам просматривать и изменять список ресурсов, публиковать собственные ресурсы и управлять файлами.
- **Разрешения Write (разрешения Read и Directory Browsing отсутствуют).** Чтобы разрешить клиентам публиковать информацию в каталог, не позволяя другим ее просматривать, установите Write (без разрешений Read и Directory Browsing). Такую конфигурацию можно применять при голосовании или передаче отзывов клиентов. При отсутствии разрешения Directory Browsing клиентским браузерам запрещается доступ к каталогу WebDAV.
- **Разрешения Read и Write (разрешения Directory Browsing отсутствуют).** Используйте эту конфигурацию, если считаете, что непонятные посторонним имена файлов обеспечат надежную защиту. Однако это скорее не метод защиты, а всего лишь одна из мер предосторожности, так как злоумышленник легко найдет нужный ему файл методом проб и ошибок.
- **Разрешение Index This Resource (Индексация каталога).** Установите это разрешение, если хотите предоставить клиентам возможность поиска ресурсов в каталоге.

Контроль доступа при помощи DACL

При создании каталога публикации WebDAV на диске с файловой системой NTFS Windows 2000 Server по умолчанию дает всем пользователем право Full Control (Полный доступ). Замените его на разрешения Read (Чтение), после чего предоставьте право Write (Запись) отдельным пользователям или группам.

Защита кода сценария

Если в каталоге публикации содержатся файлы сценариев, которые Вы не хотите показывать клиентам, можете запретить доступ к ним, отменив разрешение Script source access (Доступ к тексту сценария). Файлами сценариев считаются файлы с расширениями, включенными в список привязки приложений. Все остальные исполняемые файлы считаются

статическими файлами HTML, в том числе с расширением .exe, если для каталога не включен параметр Scripts and Executables (Сценарии и исполняемые файлы).

Чтобы .exe-файлы не рассматривались как файлы HTML и не могли загружаться клиентам, откройте диалоговое окно свойств каталога публикации, перейдите на вкладку Virtual Directory (Виртуальный каталог) и в списке Execute Permissions (Разрешен запуск) выберите Scripts and Executables (Сценарии и исполняемые файлы) (рис. 14-17).

При этом уровне разрешений доступ к исполняемым файлам зависит от параметра Script source access (Доступ к тексту сценария). Другими словами, если он включен, клиенты с правом Read (Чтение) могут просматривать все исполняемые файлы, а клиенты с правом Write (Запись) — редактировать и исполнять их. Такая конфигурация подвергает риску Ваш узел, так как программы, наносящие вред Вашему узлу, могут быть опубликованы в каталоге и запушены оттуда.

Редактировать файлы с расширениями, отсутствующими в списке Application Mapping (Сопоставление приложений), могут клиенты с правами:

- Write (Запись);
- Execute (Разрешен запуск) со значением Scripts only (Только сценарии).

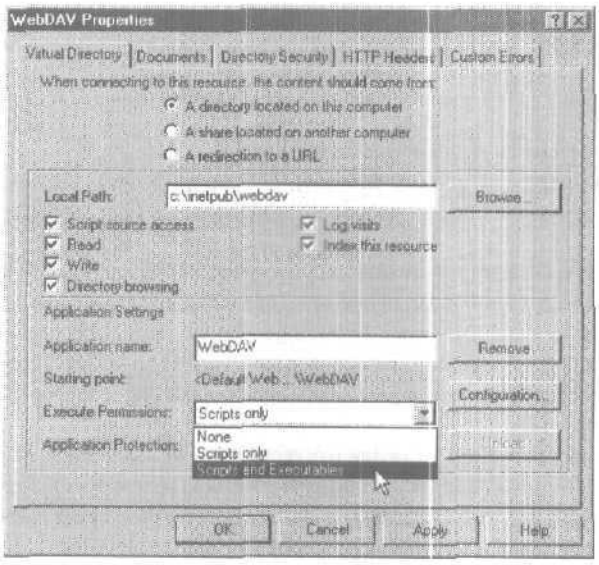


Рис. 14-17. Выбор параметра Scripts and Executables (Сценарии и исполняемые файлы) из списка Execute Permissions (Разрешен запуск)

Редактировать любые исполняемые файлы могут клиенты с разрешениями:

- Script source access (Доступ к тексту сценария);
- Execute (Разрешен запуск) со значением Scripts and Executables (Сценарии и исполняемые файлы).

Отказ в обслуживании

Для перемещения очень больших файлов в каталог WebDAV может потребоваться солидный объем дискового пространства. Чтобы ограничить его, используйте дисковые квоты.

Публикация и управление файлами

Пользователи могут подключаться к каталогу публикации WebDAV, публиковать свои документы, перетаскивая их в каталог публикации, и управлять файлами в каталоге.

Примечание Даже подключившись к серверу через брандмауэр, пользователи могут публиковать документы в каталог WebDAV, имея необходимые права и если брандмауэр разрешает публикацию.

Для подключения к каталогу публикации WebDAV с другого Windows 2000-компьютера можно использовать окно My Network Places (Мое сетевое окружение).

К каталогу WebDAV можно подключаться с любого компьютера, на котором установлены ОС Windows 2000/NT 4.0/98/95, а также Internet Explorer 5. Подключившись к этому каталогу, Вы можете выполнять те же операции по управлению файлами и публикации, что и при подключении через Windows 2000. Кроме того, для создания, публикации или сохранения документа в каталоге WebDAV можно использовать любое приложение Office 2000.

Резюме

На компьютере с Windows 2000 Server можно одновременно разместить несколько Web- и FTP-узлов. При этом пользователям будет казаться, что каждый узел находится на отдельном компьютере. Любой узел может иметь одно или несколько доменных имен. Управление узлами включает в себя ряд задач, наиболее важные из которых запуск и остановка узлов, создание узлов, задание имени узла и перезапуск IIS. Конфигурация IIS может быть заархивирована, чтобы впоследствии к ней можно было вернуться. Администрирование IIS можно производить с удаленного компьютера. WebDAV расширяет возможности протокола HTTP 1.1, позволяя клиентам публиковать, блокировать и управлять ресурсами в Web. Соединившись с каталогом WebDAV, пользователи могут легко и быстро искать в нем файлы по их содержимому или свойствам. Каталог публикации можно расположить где угодно, кроме каталога Wwwroot. Для зашиты сервера используются механизмы системы безопасности — аутентификация клиентов, контроль доступа и отказ в обслуживании. Создав каталог публикации, можно разрешить пользователям искать в нем файлы по их содержимому и свойствам. С Windows 2000-компьютера можно подключаться к каталогу публикации, расположенному на другом сервере. Также к каталогу можно подключаться с любого компьютера, на котором установлены ОС Windows 2000/NT 4.0/98/95, а также Internet Explorer 5.

Занятие 3. Настройка и запуск Telnet Services

Службы Telnet обеспечивают поддержку протокола Telnet, являющегося частью стека протоколов TCP/IP. Telnet — это протокол для подключения к удаленному компьютеру, сетевому устройству или частной сети **TCP/IP.** Доступ к удаленному компьютеру обеспечивается совместной работой Telnet Server и Telnet Client. В Windows 2000 Telnet Server по сути является службой, вследствие чего и стал называться службой Telnet. Его клиенты могут подключаться к компьютеру, на котором запушена служба Telnet, и выполнять на нем приложения, работающие в текстовом режиме. Telnet выполняет функции шлюза, через который клиенты Telnet могут связываться друг с другом. С помощью клиента Telnet пользователи могут связываться с удаленным компьютером и взаимодействовать с ним в окне терминала.

Изучив материал этого занятия, вы сможете:

- ✓ настроить службы Windows 2000 Telnet для доступа к ним клиента Telnet;
- ✓ соединяться со службой Telnet при помощи клиента Microsoft Telnet Client.

Продолжительность занятия - около 25 минут.

Службы Telnet

Используя службу Windows 2000 Telnet, клиенты Telnet могут соединяться с компьютером, на котором запущена эта служба, и выполнять на нем команды из командной строки так же, как если бы они сидели перед этим компьютером. В частности, они могут выполнять команды из командной строки, подключаться к серверу, регистрироваться на нем и выполнять приложения, работающие в текстовом режиме. Службы Telnet выполняют функции шлюза, через который клиенты Telnet могут связываться друг с другом. Максимально службы Telnet могут одновременно поддерживать 63 клиента.

Лицензирование соединений с сервером Telnet

В комплект поставки Windows 2000 Server входят две лицензии клиентских подключений Telnet. Это ограничивает число клиентов, которые одновременно могут устанавливать соединение со службой Telnet, до двух. Если Вам нужно больше лицензий, приобретите пакет Windows Services for UNIX.

Аутентификация в Telnet

Для доступа к серверу Telnet можно применять локальное имя пользователя и пароль в Windows 2000, а также учетную запись домена. Схема безопасности интегрирована в систему безопасности Windows 2000. Если Вы не выключили аутентификацию NTLM, имя пользователя и пароль будут переданы серверу Telnet в незашифрованном виде.

В случае аутентификации NTLM клиент задействует в качестве сведений для аутентификации контекст безопасности Windows 2000, и пользователю не придется вводить имя и пароль. Его имя и пароль передаются в зашифрованном виде.

Примечание Если от пользователя требуется сменить пароль при следующем входе в систему, он не сможет зарегистрироваться в службе Telnet в случае аутентификации NTLM. Сначала он должен зарегистрироваться на сервере, изменить свой пароль, а затем войти из клиента Telnet.

Запуск и остановка сервера Telnet

Telnet по умолчанию конфигурируется для ручного запуска. Настроить автоматический запуск Telnet, а также запустить и остановить ее можно из оснастки Services (Службы) или Computer Management (Управление компьютером). На рис. 14-18 показано диалоговое окно свойств службы Telnet.

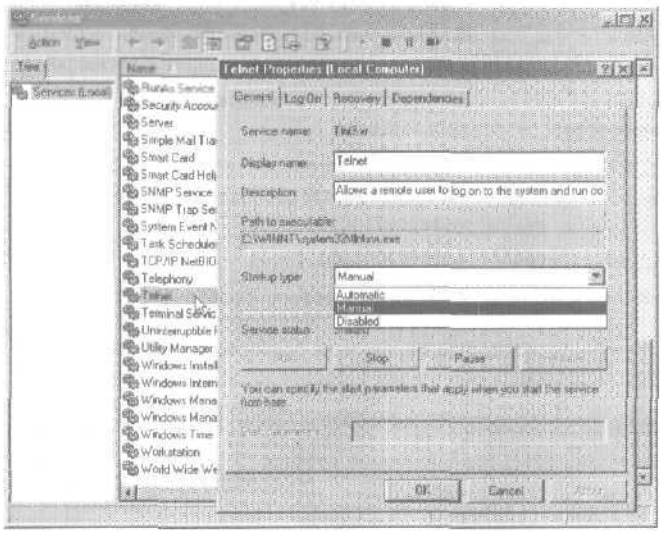


Рис. 14-18. Диалоговое окно свойств службы Telnet

Для обращения к Telnet в оснастке Computer Management (Управление компьютером) раскройте узел Services and Applications (Службы и приложения). В дереве консоли щелкните Services (Службы), а затем из списка служб в правой панели выберите Telnet.

Telnet можно запустить/остановить из командной строки: для запуска введите в командной строке **net start tlntsvr или net start telnet** и нажмите Enter, а для остановки - net stop **tlntsvr или net stop telnet** и нажмите Enter.

Утилита Telnet Server Admin

Утилита Telnet Server Admin (Управление сервером Telnet) служит для запуска и остановки сервера Telnet, для получения информации о сервере, текущих пользователях, окончания пользовательского сеанса и изменения параметров сервера Telnet, записываемых в реестр.

Внимание! Неправильное редактирование реестра может нанести серьезный вред Вашей системе. Поэтому перед внесением изменений в реестр рекомендуется заархивировать все ценные данные.

Чтобы вызвать Telnet Server Admin, щелкните значок Telnet Administration Tool (Управление сервером Telnet) в программной группе Administrative Tools (Администрирование) или, раскрыв меню Start/Run, введите **tlntadmn** и щелкните кнопку OK. Если эта утилита не запускается, возможно, она не установлена. (В этом случае Вам нужно установить пакет Adminpak.msi, об этом см. главу 6.)

Параметры утилиты Telnet Server Administration.

Параметр	Имя	Описание
0	Quit this application (Выйти из этого приложения)	Завершение работы утилиты
1	List the current users (Вывести список текущих пользователей)	Вывод списка текущих пользователей, включая имя пользователя, домен, адрес удаленного компьютера, время регистрации
2	Terminate a user session (Прервать сеанс пользователя)	Завершение сеанса выбранного пользователя
3	Display/change registry settings (Отобразить/изменить параметры реестра)	Вывод списка параметров реестра, которые Вы можете изменять (см. приведенную ниже таблицу)
4	Start the service (Запустить службу)	Запуск службы Telnet
5	Stop the service (Остановить службу)	Завершение работы службы Telnet

Утилита Telnet Server Admin позволяет изменять параметры реестра, хранящиеся в разделе HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\TelnetServer\1.0 (рис. 14-19).

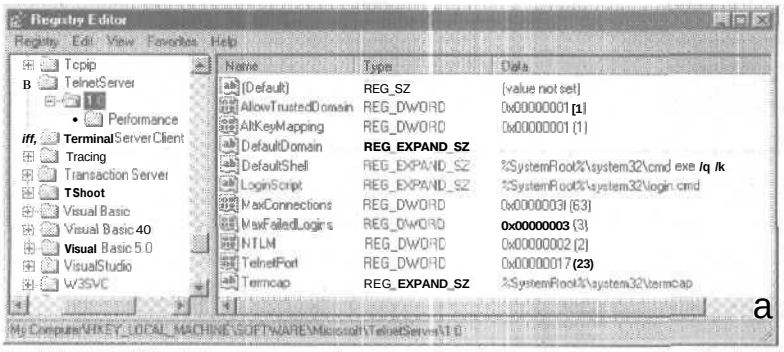


Рис. 14-19. Параметры сервера Telnet в реестре, изменяемые утилитой Telnet Server Admin

Параметры сервера Telnet в реестре, которые Вы можете изменить.

Параметр	Имя	Описание	Значение по умолчанию
1	AllowTrusted-Domain	Изменение текущего значения доверенного домена	1
2	AltKeyMapping	Изменение текущего значения	1
3	Default Domain	Задание имени домена по умолчанию	. (точка означает текущий домен сервера Telnet)
4	DefaultShell	Путь к исполняемому файлу оболочки	%systemroot%\System32\ Cmd.exe /q /k. Переключатель /q отключает эхо, а /k — выполняет команду, но не закрывает командное окно.

(окончание)

Параметр	Имя	Описание	Значение по умолчанию
5	LogonScript	Путь и имя файла глобального сценария регистрации клиента. По умолчанию этот файл привязывает клиента Telnet к его домашнему каталогу, если последний указан в профиле пользователя.	%systemroot%\System32\ login.cmd
6	Max Failed Logins	Максимально допустимое число неудачных попыток входа (когда лимит будет превышен, сеанс завершится)	3
7	NTLM	Текущее количество пользователей, прошедших аутентификацию NTLM	2
8	TelnetPort	Заданный по умолчанию порт сервера Telnet	23

Примечание В параметре реестра Termcap указано расположение файла Termcap (Terminal Capabilities), используемого рядом клиентских утилит для определения порядка перемещения курсора во время терминального сеанса.

Изменение заданной по умолчанию учетной записи домена вступает в силу после перезапуска службы Telnet. С утилитой Telnet Server Administration могут работать лишь члены группы Administrators.

Устранение неполадок

Наиболее распространенные проблемы, которые могут возникнуть при работе сервера Telnet, таковы:

Сообщение об ошибке	Причина проблемы	Решение проблемы
Неправильный ввод.	Введено недопустимое значение.	Измените промежуток возможных значений параметра и повторите ввод.
Не удается открыть нужный раздел реестра.	Для открытия раздела реестра сервер Telnet должен быть запущен. Поэтому возникновение ошибки означает, что сервер не работает.	Запустите службу Telnet.
Не удается получить значение из реестра.	Для запроса значения из реестра сервер Telnet должен быть запущен. Поэтому возникновение ошибки означает, что сервер не работает.	Запустите службу Telnet.

Клиент Telnet

Для соединения с удаленным компьютером, на котором работают службы Telnet или другие приложения сервера Telnet, используется Microsoft Telnet Client. Установив соединение, можно взаимодействовать с сервером Telnet. Тип устанавливаемого сеанса связи зависит от конфигурации службы Telnet. Типичные примеры ее использования — общение, игры, администрирование системы и симуляция локального входа.

С удаленным компьютером клиент Telnet соединяется по протоколу Telnet, являющемуся частью набора протоколов TCP/IP. ПО клиента Telnet, входящего в Windows 2000, позволяет устанавливать соединение с удаленным компьютером, регистрироваться на нем и взаимодействовать с ним. Пользователи предыдущих версий клиента Microsoft Telnet обратят внимание на некоторые особенности новой версии. Так, Microsoft Telnet Client перестал быть приложением Windows, став приложением, запускаемым из командной строки. Это сближает его с клиентами Telnet для UNIX.

Важное нововведение в Microsoft Telnet Client — поддержка аутентификации NTLM, применяемая при подключении клиента Telnet к компьютеру с Windows 2000, на котором запушена служба Telnet.

Примечание Microsoft Telnet Client не поддерживает ведение журнала сеанса Telnet.

Использование Telnet

Для запуска Telnet в меню Start (Пуск) выберите команду Run (Выполнить) и в поле Open (Открыть) введите **telnet.** Можно также ввести **telnet** в командной строке. Для работы с Telnet на компьютере должен быть настроен протокол TCP/IP. Кроме того, Вы должны иметь учетную запись на удаленном компьютере.

Для просмотра справки по Telnet введите **help** в командной строке Microsoft Telnet. Для соединения с узлом введите **connect** *<имя_компьютера>*, где *<имя_компьютера>* — IP-адрес или имя компьютера со службой Telnet.

Упражнение 2: настройка и подключение к службе Telnet

Настройте службу Telnet для запуска на ServerOl, затем подключитесь к службе Telnet с ServerOl и проверьте соединение. Выполняйте упражнение на ServerOl.

Примечание Второй этап упражнения можно выполнять на Server02.

► **Задание 1: включите и настройте службы Telnet**

Настройте автоматический запуск службы Telnet и запустите ее.

1. Зарегистрируйтесь на ServerOl как Administrator (Администратор) с паролем **password.**
2. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Services (Службы).

   Откроется консоль Services (Службы),
3. Дважды щелкните значок Telnet на правой панели.

   Откроется диалоговое окно Telnet Properties (Local Computer) [Telnet (Локальный компьютер) — свойства].
4. В списке Startup Type (Тип запуска) вместо Manual (Вручную) выберите Automatic (Авто).
5. Щелкните кнопку Start под заголовком Service status (Состояние).

На короткое время (пока запускается служба Telnet) откроется окно Service Control (Управление службой).

6. Щелкните кнопку OK, чтобы закрыть диалоговое окно свойств службы Telnet.
7. Закройте консоль Services (Службы).

▶ Задание 2: задействуйте Microsoft Telnet Client

Соединитесь со службой Telnet из Microsoft Telnet Client. Этот этап можно выполнять как на Server01, так и на Server02. Использование Server02 позволяет осуществить удаленный доступ к ServerOl, хотя для учебных целей приемлемо выполнять команды на ServerOl. Выбрав Server02, зарегистрируйтесь на нем как Administrator (Администратор).

1. В меню Start (Пуск) выберите команду Run (Выполнить).
   Откроется диалоговое окно Run (Запуск программы).
2. В поле Open (Открыть) введите **telnet** и щелкните кнопку OK.
   Откроется командная строка Microsoft Telnet.
3. Введите в командной строке **help или ?.**
   Вы увидите список имеющихся команд.
4. Введите **open server01.**
   Вас поприветствует сервер Telnet.

Примечание При вводе команд можно использовать сокращения. Например, вместо команды **open serverOl** можно ввести ее краткий эквивалент — **o serverOl,**

---

5. Все команды, которые могут быть введены в командную строку на ServerOl, можно выполнить и из оболочки Telnet.
6. Не завершайте сеанс связи с Telnet — он понадобится Вам далее.

▶ Задание 3: проследите за клиентскими соединениями

Используя утилиту Telnet Server Administrator, проследите за клиентскими соединениями со службой Telnet и завершите клиентское соединение.

1. В меню Start (Пуск) выберите команду Run (Выполнить).
   Откроется диалоговое окно Run (Запуск программы).
2. В поле Open (Открыть) введите **tlntadmn** и щелкните кнопку OK.
   Откроется окно утилиты Telnet Server Admin.
3. Введите 1 для вывода списка текущих пользователей.
   Появится статистика о пользователе-администраторе.
4. Введите 2 для завершения пользовательского сеанса.
   Вас попросят ввести идентификатор пользовательского сеанса, который необходимо завершить.
5. Введите 1 (идентификатор Вашего пользовательского сеанса),
   Вы снова увидите список доступных команд.
6. Перейдите в окно клиента Microsoft Telnet на ServerOl или Server02.
   Обратите внимание, что соединение с хостом прекращено.
7. Нажмите любую клавишу.
   Вы вернетесь в окно Microsoft Telnet Client.
8. Закройте это окно, введя **q** или **quit** в командную строку.
9. Вернитесь в командное окно Telnet Server Administrator.
10. Введите 0, чтобы закрыть Telnet Server Administrator.

Резюме

Доступ к удаленному компьютеру обеспечивается совместной работой Telnet Server и Telnet Client, Используя службу Windows 2000 Telnet, клиенты Telnet могут соединяться с удаленным компьютером, на котором запушена служба Telnet, и выполнять на нем команды из командной строки. Запускать и остановливать Telnet можно из оснасток Services или Computer Management и из командной строки. Для этих целей, а также для получения сведений о Telnet служит и утилита Telnet Server Admin. Она также позволяет просматривать список текущих пользователей, завершать пользовательский сеанс и изменять параметры сервера Telnet, записываемые в реестр. Для соединения с удаленным компьютером, на котором работают приложения сервера Telnet, используется Microsoft Telnet Client. Клиент Microsoft Telnet и служба Microsoft Telnet поддерживают аутентификацию NTLM. Служба Telnet обеспечивает поддержку протокола Telnet — протокола удаленного доступа, используемого для подключения к удаленному компьютеру, сетевому устройству или частной сети.

Занятие 4. Установка и настройка служб Terminal Services

Службы Terminal Services обеспечивают клиентским компьютерам доступ к Windows 2000 и новейшим версиям Windows-приложений. Любой клиент, поддерживающий службы Terminal Services, получает с их помощью доступ к Вашему рабочему столу и установленным у Вас приложениям. Встроенные в Windows 2000 службы Terminal Services обеспечивают более гибкий механизм развертывания приложений, позволяют снизить издержки управления информационными системами и удаленно управлять сетевыми ресурсами.

Изучив материал этого занятия, вы сможете:

- ✓ развернуть Terminal Services в среде Windows 2000.

Продолжительность занятия — около 40 минут.

Общие сведения о службах Terminal Services

Службы Terminal Services, выполняющиеся на Windows 2000 Server, позволяют клиентам выполнять приложения, обрабатывать и хранить данные на сервере. Они предоставляют доступ к рабочему столу сервера при помощи ПО эмуляции терминала. Это ПО может быть установлено на персональном компьютере, карманном компьютере с ОС Windows CE или терминале.

Службы Terminal Services работают следующим образом. При помощи ПО эмуляции терминала клиент передает нажатия клавиш и перемещения мыши на сервер. Службы Terminal Services обрабатывают данные на сервере и возвращают клиенту изображение экрана. Такой подход позволяет удаленно управлять сервером и централизованно управлять приложениями при минимальных требованиях к пропускной способности сетевого соединения между сервером и клиентом.

Пользователи могут подключаться к службам Terminal Services через любое соединение TCP/IP, включая удаленный доступ, Ethernet, Интернет, беспроводные сети, ГВС или *виртуальную частную сеть* (virtual private network, VPN). Возможности пользователя ограничены лишь скоростью соединения, а безопасность соединения регулируется реализацией TCP/IP в центре обработки данных.

Службы Terminal Services позволяют удаленно управлять сетевыми ресурсами и предоставляют однородный интерфейс пользователям, работающим в удаленных от головного офиса подразделениях организации, и графический интерфейс для бизнес-приложений на компьютерах с алфавитно-цифровыми дисплеями.

Службы Terminal Services встроены в Windows 2000. Их можно развернуть на сервере в режиме удаленного администрирования (Remote Administration) или в режиме сервера приложений (Application Server).

Режим удаленного администрирования

Это мощный механизм удаленного управления любым компьютером с Windows 2000 Server через любое соединение TCP/IP. Он позволяет управлять совместным доступом к файлам и принтерам, редактировать реестр с другого компьютера в сети и др. Режим удаленного администрирования позволяет управлять серверами, не совместимыми с режимом сервера приложений служб Terminal Services (например кластерной службой).

В этом режиме устанавливаются только компоненты удаленного доступа служб Terminal Services, а компоненты совместного доступа к приложениям — нет, Это позволяет снизить нагрузку на критически важные серверы. В режиме удаленного администрирования службы Terminal Services поддерживают максимум два соединения. Для них не требуется дополнительного лицензирования, поэтому сервер лицензирования Вам не нужен.

Примечание Подробнее об удаленном администрировании см. документ \chapt14\articles\TSRemote.doc на прилагаемом компакт-диске.

Режим сервера приложений

Обеспечивает централизованное развертывание и управление приложениями, сокращая затраты времени на их разработку, развертывание, обслуживание и обновление. Приложение, развернутое в Terminal Services, доступно клиентам через соединения удаленного доступа, ЛВС, ГВС и другие типы соединений.

Приложения на сервер со службами Terminal Services можно установить как напрямую, так и с удаленного компьютера. Например, опубликовать установочные пакеты Windows Installer на сервер или группу серверов со службами Terminal Services позволяют оснастка Group Policy и Active Directory. Эти приложения могут установить только пользователи с учетной записью Administrator и только отдельно на каждый сервер при условии, что в оснастке Group Policy включен соответствующий параметр.

При развертывании терминального сервера в режиме сервера приложений необходимо произвести лицензирование клиентов. Любой клиентский компьютер независимо от протокола, используемого для соединения с терминальным сервером, должен иметь лицензии служб терминалов и клиента Windows 2000.

Примечание Подробнее **об оптимизации приложений для Windows** 2000 **Terminal Services см. документ** \chapt14\articles\TSAppDev.doc на **прилагаемом компакт-диске.**

Средства администрирования

Для облегчения процесса установки служб Terminal Services для Windows 2000 в программную группу Administrative Tools (Администрирование) были добавлены такие средства администрирования, как Terminal Services Client Creator (Создатель клиента служб терминалов), Terminal Services Manager (Диспетчер служб терминалов). Terminal Services Configuration (Настройка служб терминалов) и Terminal Services Licensing (Лицензирование служб терминалов).

Примечание Terminal Services Licensing устанавливается, если выбран режим сервера приложений и установлен пакет Adminpak.msi.

Terminal Services Client Creator

Позволяет создавать диски для установки клиентского ПО Terminal Services Client на платформы Windows for Workgroups/95/98/NT.

Terminal Services Manager

Позволяет управлять всеми серверами Windows 2000, на которых работают службы Terminal Services. В частности, с его помощью администраторы могут просматривать информацию

о текущих пользователях, серверах и процессах, посылать сообщения пользователям, применять функцию удаленного управления и завершать процессы. На рис. 14-20 изображено окно консоли диспетчера служб терминалов.

Terminal **Services Configuration**

Предназначен для настройки протокола **RDP** (Remote Desktop Protocol). Изменение параметров этим инструментом носит глобальный характер (если они не наследуют значения аналогичных параметров пользовательской конфигурации). К их числу относятся параметры шифрования соединения и входа в систему, время ожидания, программы, автоматически запускаемые при успешном входе в систему, параметры удаленного управления сеансом, отображения принтеров Windows, портов LPT и буферов обмена, а также применение этих параметров к конкретной сетевой плате.

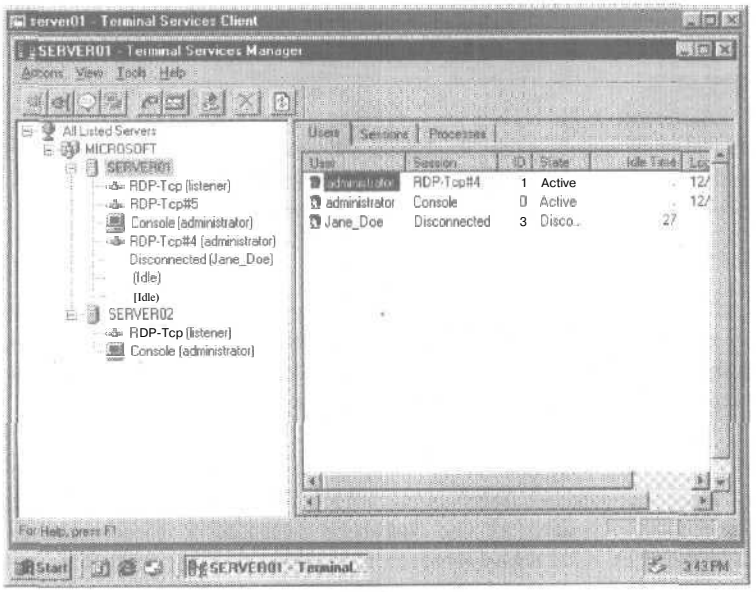


Рис. 14-20. Управление службами Terminal Services на Server01 с помощью Terminal Services Manager (Диспетчер служб терминалов)

Terminal Services Licensing

Позволяет хранить и отслеживать сведения о лицензиях клиентов Windows 2000 Terminal Services. Этот инструмент может быть установлен во время обшей установки служб Terminal Services или после. При подключении клиента к службам терминалов проверяется его лицензия. Если ее нет или требуется ее обновление, терминальный сервер обращается к *серверу лицензий* (license server), который выбирает лицензию из пула имеющихся лицензий, и передает ее клиенту. Если свободных лицензий нет, сервер лицензий предоставляет клиенту временную лицензию. После этого лицензия каждого клиента ставится в соответствие определенному компьютеру или терминалу.

Примечание О средствах администрирования Terminal Services см. документ \chapt14\articles\TSsol.doc на прилагаемом компакт-диске.

Компоненты лицензирования Terminal Services

Службы Terminal Services по-своему лицензируют подключающихся к ним клиентов. Этот метод не зависит от лицензирования клиентов Windows 2000 Server. Существует четыре компонента лицензирования служб Terminal Services: Microsoft Clearinghouse, сервер лицензий, сервер терминалов и клиентские лицензии.

Microsoft Clearinghouse

Microsoft Clearinghouse — это БД, созданная Microsoft, для запуска сервера лицензий и установки на него ключевого пакета клиентской лицензии, Она хранит сведения об активизированных серверах лицензий и выданных им ключевых пакетах. Это поможет записать в журнал использование клиентами серверов терминалов в организации и убедиться в том, что куплено необходимое число клиентских лицензий. Доступ к БД Microsoft Clearinghouse можно получить из оснастки Terminal Services Licensing.

Сервер лицензий

Хранит все лицензии, установленные на сервер терминалов, и записывает выдачу лицензий клиентским компьютерам или терминалам. До начала выдачи лицензий клиентам сервер терминалов надо подключить к активизированному серверу лицензий, Один сервер лицензий может одновременно работать с несколькими серверами терминалов.

Сервер терминалов

Это сервер, на котором включены службы терминалов. Он обеспечивает доступ к приложениям Windows, запущенным на сервере, и поддерживает сеансы нескольких клиентов. При входе клиентов сервер терминалов проверяет действительность лицензий клиентов. Если лицензии нет, сервер терминалов запрашивает ее на сервере лицензий.

Клиентские лицензии

Каждый компьютер- или терминал-клиент, подключенный к серверу терминалов, должен иметь действительную клиентскую лицензию. Она хранится локально и представляется серверу терминалов при каждом подключении клиента к серверу. Сервер проверяет лицензию и затем позволяет клиенту выполнить подключение.

Примечание Подробнее о лицензировании в службах Terminal Services см. документ \chapt14\articles\TSLicensing.doc на прилагаемом компакт-диске.

Администрирование сервера лицензий

Развертывание сервера лицензий служб терминалов состоит из установки сервера лицензий, его включения и активизации и установки лицензий.

Установка сервера лицензий

Для работы терминальных служб в режиме сервера приложений нужен сервер лицензий. Служба лицензирования хранит и отслеживает сведения о лицензиях, выданных клиентским компьютерам и терминалам для доступа к серверу терминалов.

Сервер лицензий активируется через Microsoft Clearinghouse. В его состав входят *лицензии клиентского доступа* (Client Access Licenses) для распространения лицензий, хранящихся в БД Clearinghouse. Сервер лицензий используется сервером служб Terminal Services

только для выпуска новых лицензий, поэтому перед ним стоит лишь одна задача — извлечь лицензии из БД Clearinghouse.

Включение сервера лицензий

Служба лицензирования Terminal Services может быть включена при запуске Windows 2000 Server Setup. При развертывании служб терминалов на крупном предприятии рекомендуется устанавливать сервер терминалов на рядовой сервер домена или на изолированный сервер. Нежелательно устанавливать сервер лицензий и сервер терминалов на один компьютер, так как службы терминалов требуют много ресурсов.

Существует два типа серверов лицензий: доменный сервер лицензий и коммерческий сервер лицензий. Перед установкой решите, какой больше подходит.

- **Доменный сервер лицензий.** Выберите этот тип, если хотите иметь отдельный сервер лицензий для каждого домена. В сети, где есть рабочие группы или домены Windows NT 4.0 можно установить только доменные серверы лицензий. Службы терминалов могут обращаться только к серверам лицензий, расположенным в их домене. Этот тип серверов лицензий устанавливается по умолчанию.
- **Коммерческий сервер лицензий** может обслуживать серверы служб терминалов, находящиеся в любом домене узла (но обязательно в том же узле), при условии, что это домен Windows 2000. Этот тип серверов следует использовать при наличии в сети большого количества доменов. Коммерческие серверы лицензий нельзя установить одновременно с Windows 2000. Для этого служит утилита Add/Remove Programs.

Для выбора физического местоположения сервера лицензий примите во внимание то, как сервер служб Terminal Services обнаруживает его и связывается с ним. При включении служб терминалов сервер опрашивает службы домена и Active Directory для поиска сервера лицензий. (В рабочих группах сервер терминалов производит широковещательную рассылку по всем серверам рабочей группы, находящимся в той же подсети.)

Примечание В доменах Windows 2000 сервер лицензий должен быть установлен на контроллер домена. В рабочих группах или доменах Windows NT 4.0 его можно установить на любой сервер. Если в будущем Вы планируете перейти с домена рабочих групп или Windows NT 4.0 к домену Windows 2000, установите сервер лицензий на компьютер, который станет контроллером домена Windows 2000.

Для активизации сервера лицензий и доступа к БД Clearinghouse через Интернет установите сервер на компьютере, имеющем доступ в Интернет.

Сервер лицензий Windows 2000 нужно включить не позднее, чем через 90 дней с момента включения служб терминалов Windows 2000. Если в течение этого срока службу лицензирования не включить, службы терминалов перестанут работать.

Активизация сервера лицензий

Чтобы сервер лицензий мог быть идентифицирован серверами терминалов и выпускать для них лицензии, его необходимо активизировать при помощи мастера лицензирования.

Сервер лицензий можно активизировать:

- через Интернет;
- с помощью Web-браузера;
- по факсу;
- по телефону.

Если компьютер, на котором установлена оснастка Terminal Services Licensing, подключен к Интернету, активизация сервера лицензий через Интернет — самый легкий и быстрый способ. Мастер направит Вас на безопасный Интернет-узел Microsoft, где происходит активизация серверов лицензий. При этом Microsoft предоставит ему цифровой сертификат, удостоверяющий владельца сервера. Используя его, сервер лицензий может впоследствии запрашивать у Microsoft лицензии клиентского доступа для Ваших терминальных серверов.

Если компьютер с сервером лицензий не подключен к Интернету, но есть доступ к WWW через браузер, установленный на другом компьютере, можно активизировать сервер лицензий с помощью Web-браузера. Механизм активизации здесь такой же, как и в предыдущем случае — мастер направляет Вас на безопасный Интернет-узел Microsoft, где Вы получаете сертификат для сервера лицензий.

Можно активизировать сервер лицензий, послав информацию по факсу или позвонив в ближайший *центр поддержки клиентов* (Customer Support Center, CSC). Найти номер соответствующего телефона или факса также поможет мастер. При использовании первого из этих методов активизации Microsoft вышлет Вам по факсу подтверждение Вашего запроса. Во втором случае Вы передадите свой запрос представителю службы технической поддержки по телефону.

Сервер лицензий должен быть активизирован только раз. Пока процесс активизации не завершен, сервер лицензий может выдавать временные лицензии. Клиенты могут пользоваться ими не более 90 дней.

Цифровой сертификат, идентифицирующий ваш сервер лицензий, хранится в виде *идентификатора сервера лицензий* (License Server ID). Храните копию этого номера в безопасном месте. Для просмотра активизированного сервера лицензий в оснастке Terminal Services Licensing выделите нужный сервер и в меню View (Вид) выберите команду Properties (Свойства). В качестве способа связи выберите WWW и щелкните кнопку OK. Затем в меню Action выберите команду Install Licenses (Установить лицензии). В окне мастера лицензирования Вы увидите идентификационный номер сервера лицензий.

Установка лицензий

Чтобы разрешить настройку коннектора Интернета и открыть постоянный доступ к серверу служб терминалов пользователям — не клиентам Windows 2000, необходимо установить лицензии служб терминалов. Клиентские лицензии доступа к службам терминалов и лицензии Internet Connector можно приобрести так же, как и любое ПО. Установить их поможет мастер Licensing (Мастер лицензирования).

После того, как лицензии были установлены, сервер лицензий начнет их развертывание. Клиенты с временными 90-дневными лицензиями получат лицензии доступа при своем следующем подключении (если число временных лицензий не превысит число установленных клиентских лицензий).

Развертывание служб терминалов на клиентских компьютерах

Клиентские компьютеры и терминалы соединяются с терминальным сервером с помощью небольшой клиентской программы, хранимой на диске или в ПЗУ. Выбор клиентской платформы зависит от имеющейся базы и индивидуальных потребностей пользователя. Минимальные требования, которым должен удовлетворять клиентский компьютер или терминал для соединения с сервером служб терминалов, — это возможность установки на нем клиентского ПО и сетевое подключение.

Клиентские компьютеры с ОС Windows для подключения к службам Terminal Services должны иметь минимум микропроцессор с частотой 33 МГц (рекомендуется конфигурация 486/66), 16-разрядную видеоплату VGA и стек протоколов Microsoft TCP/IP. Клиент служб терминалов может иметь ОС Windows for Workgroups 3.11/95/98/NT 3.51 или более позднюю версию, а также Windows 2000.

Клиент служб терминалов занимает всего 500 кб на диске и около 4 Мб оперативной памяти при своем выполнении. Если включена функция кэширования экрана, потребуется еще 10 Мб на диске. Объем ОЗУ компьютера с клиентом служб терминалов, необходимый для достижения оптимальной производительности, варьируется в зависимости от ОС. Так, для Windows for Workgroups 3.11/95 он составляет 8 Мб, для Windows 98 — 24 Мб, для Windows 2000 - 32 Мб.

Примечание Клиент служб терминалов для устройств Windows CE находится на установочном компакт-диске Windows 2000 Server в папке \Valueadd\msft\mgmt\mstsc_hpc.

ПО клиента RDP устанавливается по умолчанию в качестве одного из компонентов служб терминалов. Различные клиенты устанавливаются в папку %systemroot%\system32\clients\tsclient.

Установить клиентское ПО можно:

- создав сетевой файл и произведя установку через сеть;
- создав клиентский образ, щелкнув в программной группе Administrative Tools (Администрирование) ярлык Terminal Services Client Creator (Создатель клиента служб терминалов); этот клиентский образ можно потом установить с дискеты.

Примечание Для соединения с сервером клиентам служб Terminal Services необходим протокол TCP/IP, однако сами службы Terminal Services могут соединяться с серверами Novell по протоколу IPX.

Конфигурации клиентов

Чтобы повысить производительность служб терминалов:

- отключите интерфейс Active Desktop;
- отключите плавную прокрутку;
- избегайте использования графики и эффектов анимации, в том числе анимированных рисунков, заставок экрана, мигающих курсоров и анимированного помощника Microsoft Office; размещайте ярлыки на рабочем столе и старайтесь сделать структуру меню Programs (Программы) как можно более «плоской». Не украшайте рабочий стол рисунками — в окне Display Properties (Свойства: Экран) перейдите на вкладку Background (Фон) и отключите фоновый рисунок;
- разрешите совместное использование файлов на клиентском компьютере и присвойте общим дискам легко узнаваемые имена, например «drivec», в то же время не забывая о системе безопасности;
- не запускайте приложения MS-DOS или Win16 (16-разрядные);
- сконфигурируйте сервер служб Terminal Services так, чтобы функции NetBIOS возвращалось имя пользователя, а не имя компьютера;
- обучите пользователей комбинациям «горячих клавиш», применяемым в клиентском сеансе связи со службами терминалов (эти комбинации несколько отличаются от комбинаций «горячих клавиш» в Windows 2000).

Обновление до Terminal Services

Механизм обновления зависит от текущей настройки этих служб.

Переход с WinFrame (с/без MetaFrame)

Прямой переход от WinFrame к службам терминалов невозможен. Сначала нужно перейти от WinFrame к Microsoft Terminal Server 4.0, а от него — к Windows 2000.

Terminal Server 4.0 без MetaFrame

От Terminal Server 4.0 можно перейти к службам терминалов за один шаг. При установке Windows 2000 сервер обнаруживает Terminal Server 4.0 и автоматически выполняет обновление (при этом службы терминалов переводятся в режим сервера приложений). Если Вы установите службы терминалов в режиме сервера приложений, придется переустановить существующие приложения.

Terminal Server 4.0 с MetaFrame

Переход от Terminal Server 4.0 с MetaFrame к службам терминалов аналогичен процессу перехода от Terminal Server 4.0 без MetaFrame. Разница лишь в том, что сначала нужно перейти к версии MetaFrame для Windows 2000.

Windows NT без служб терминалов

Чтобы установить службы терминалов, во время установки Windows 2000 выберите Terminal Services в режиме удаленного администрирования или в режиме сервера приложений.

Установка и настройка приложений

Сервер Windows 2000 со службами терминалов в режиме сервера приложений поддерживает многопользовательский доступ к любому числу приложений.

Для установки и удаления приложений служит утилита Add/Remove Programs на панели управления Windows. Существует и более простой способ установки приложений – перевести сервер в режим установки. Для этого введите в командной строке **change** user / **install.** По завершении установки ПО введите **change user /execute** для возврата сервера в режим выполнения (execute).

Утилита Add/Remove Programs не требует ввода команды смены пользователя (change user), так как она выполняет ее автоматически. Поэтому, а также потому, что при вводе команд в командную строку возможны ошибки, этот метод установки более предпочтителен. Если при установке приложения не использовались ни утилита Add/Remove Programs, ни включенный в командной строки режим установки, его следует удалить и повторно установить.

Устанавливать приложения на сервер служб терминалов вправе администраторы.

Развертывание приложений из оснастки Group Policy

Службы Active Directory и оснастка Group Policy предоставляют гибкий механизм развертывания приложений при помощи Windows Installer. Существует несколько способов установки приложений и управления ими:

- установка пользователем на локальный компьютер;
- назначение приложения пользователю или компьютеру системным администратором с контроллера домена;

- публикация приложения пользователю системным администратором с контроллера домена.

Чтобы установить приложение при помощи Windows Installer, необходимо иметь установочный пакет этого приложения (файл с расширением .MSI).

Развертывание приложений с контроллера домена

Чтобы развернуть приложение с контроллера домена, системный администратор должен запустить соответствующее MSI-приложение. Серверы приложений не могут назначать или публиковать приложения пользователям.

Если при первоначальной установке на локальный диск были установлены не все необходимые компоненты приложения, надо использовать *файлы преобразования* (transform files), позволяющие выбрать устанавливаемые компоненты.

Администратор может установить приложение и через сеанс удаленной связи или консоль сервера приложений. При этом для типичной установки используется команда

```
Msiexec/I имя_приложения.MSI
TRANSFORMS=имя_файла_преобразования.MST
ALLUSERS=1
```

Установка приложения в многопользовательской среде отличается от установки приложения на компьютер отдельного пользователя. При установке ПО на сервер приложений функционирующая система не должна подвергаться риску, кроме того, должен поддерживаться многопользовательский доступ. Поэтому устанавливать приложения в этом случае могут только администраторы.

Системный администратор должен решать, какие приложения установить, а также гарантировать, что перед началом пользовательских сеансов связи все приложения установлены на локальные компьютеры пользователей и работают.

Упражнение 3: установка и конфигурирование Terminal Services и Terminal Services Licensing

Установите службы Windows 2000 Terminal Services и выполните их удаленную настройку с Server02. Затем установите службы лицензирования и откройте сеанс связи с терминальными службами с Server02.

▶ Задание 1: установите службы Terminal Services и запустите их в режиме удаленного администрирования

Установите службы Terminal Services на Server01 и запустите их в режиме удаленного администрирования. Затем произведите удаленное администрирование этих служб с Server02. Удостоверьтесь, что установочный компакт-диск Windows 2000 Server вставлен в привод CD-ROM на Server01.

1. Зарегистрируйтесь на ServerOl как Administrator (Администратор) с паролем **password.**
2. Раскройте меню Start\ Settings (Пуск\Настройка) и щелкните ярлык Control Panel (Панель управления).
3. Дважды щелкните значок Add/Remove Programs.

   Откроется одноименное диалоговое окно.
4. Щелкните кнопку Add/Remove Windows Components (Установка и удаление компонентов Windows).

   Откроется окно мастера компонентов Windows.

5. Пометьте флажок Terminal Services (Службы терминалов) и щелкните кнопку Next (Далее).

   Откроется окно Terminal Services Setup (Установка служб терминалов).

6. Прочитав информацию в этом окне и убедившись, что выбран переключатель Remote Administration Mode (Режим удаленного управления), шелкните кнопку Next (Далее).

   Откроется окно Configuring Components (Настройка компонентов), а затем — окно Completing the Windows Components Wizard (Завершение работы мастера компонентов Windows).

7. Щелкните кнопку Finish (Готово).

   Вы снова увидите диалоговое окно Add/Remove Programs,

8. Щелкните кнопку Close (Закрыть) и закройте панель управления.

   Появится сообщение, что для вступления изменений в силу надо перезагрузить компьютер.

9. Щелкните кнопку Yes (Да), чтобы перезагрузить компьютер.
10. Не входите в систему с Server01 после его перезагрузки. Вы войдете с Server02, используя режим удаленного администрирования служб Terminal Services.
11. С Server02 зарегистрируйтесь на ServerOl как Administrator с паролем password. Убедитесь, что Вы зарегистрировались в домене MICROSOFT.
12. В меню Start (Пуск) выберите команду Run (Выполнить).

    Откроется диалоговое окно Run (Запуск программы).

13. В поле Open (Открыть) введите **\\server01\c$\Program Files\terminal** services **client** и щелкните кнопку OK.

    Откроется окно Terminal Services Client.

14. Дважды щелкните значок Conman.

    Откроется окно Client Connection Manager (Диспетчер клиентских подключений).

15. Щелкните первый значок на панели инструментов.

    Запустится мастер Client Connection Manager (Мастер клиентских подключений).

16. Щелкните кнопку Next (Далее).

    Откроется окно Create A Connection (Создание подключения).

17. В поле Connection Name (Имя подключения) введите **ServerOl Remote Administration.**
18. В поле Server name or IP Address (Имя или IP-адрес сервера) введите **ServerOl и** щелкните кнопку Next (Далее).

    Откроется окно Automatic Logon (Автоматический вход).

19. Пометьте флажок Logon Automatically With This Information (Автоматический вход со следующими параметрами).
20. В поле User Name (Пользователь) введите **administrator** (Администратор).
21. В поле Password (Пароль) введите **password.**
22. В поле Domain (Домен) введите **microsoft** и щелкните кнопку Next.

    Откроется окно Screen options (Параметры экрана).

23. Выберите разрешение монитора, поддерживаемое Server02. Если Вы не знаете, какое разрешение он поддерживает, щелкните переключатель 640 x 480.
24. Щелкните кнопку Next (Далее).

    Откроется окно Connection Properties (Свойства подключения).

25. Пометьте флажки Enable Data Compression (Включить сжатие данных) и Cache Bitmaps (Кэширование точечных рисунков) и щелкните кнопку Next (Далее).

    Откроется окно Starting A Program (Запуск программы).

26. Щелкните кнопку Next (Далее).

    Откроется окно Icon And Program Group (Значок и группа программ).

27. Щелкните кнопку Next (Далее).

    Откроется окно Completing The Client Connection Manager Wizard (Завершение работы мастера клиентских подключений).

28. Щелкните кнопку Finish (Готово).

    Откроется окно Client Connection Manager (Диспетчер клиентских подключений), в котором Вы увидите созданное соединение.

29. Дважды щелкните значок Server01 Remote Administration.

    Откроется окно Connecting (Подключение), а затем — окно служб Terminal Services с заголовком SERVER01 — Terminal Services Client (ServerOl Remote Administration).

30. В диалоговом окне Log On To Windows (Вход в Windows) введите **password и** щелкните кнопку OK.

    Теперь с Server02 Вы можете удаленно управлять Server01. Посмотрите на экран ServerOl и обратите внимание, что этот компьютер не зарегистрирован в сети, хотя Вы зарегистрировались на нем с Server02.

31. Закройте окно SERVER01 — Terminal Services Client (Server01 Remote Administration) на Server02.

    Появится сообщение, что сейчас Вы закончите соединение с Server01, но можете возобновить сеанс позднее и продолжить выполнение программ, запущенных в этом сеансе.

32. Щелкните кнопку OK.

33. Закройте утилиту Client Connection Manager (Диспетчер клиентских подключений), а затем — окно Terminal Services Client.

▶ Задание 2: установите службы лицензирования

Установите на ServerOl службы лицензирования, необходимые серверу приложений. Убедитесь, что установочный компакт-диск Windows 2000 Server вставлен в привод CD-ROM на Server01.

Примечание При развертывании служб терминалов на крупном предприятии не рекомендуется устанавливать службы лицензирования на компьютер со службами терминалов в режиме сервера приложений.

---

1. Зарегистрируйтесь на ServerOl как Administrator (Администратор) с паролем password.
2. Раскройте меню Start\Settings и щелкните ярлык Control Panel.
3. Дважды щелкните значок Add/Remove Programs (Установка и удаление программ).

   Откроется одноименное диалоговое окно.

4. Щелкните кнопку Add/Remove Windows Components.

   Откроется окно мастера компонентов Windows.

5. Пометьте флажок Terminal Services Licensing (Лицензирование служб терминалов) и щелкните кнопку Next (Далее).

   Откроется окно Terminal Services Licensing Setup.

6. Щелкните переключатель Application Server Mode (Режим сервера приложений) и кнопку Next (Далее).

   Появится сообщение, что после установки средства администрирования Windows 2000 могут работать некорректно.

7. Щелкните кнопку Next (Далее).
   Откроется окно Terminal Services Licensing Setup.
8. Щелкните переключатель Your Entire Enterprise (Всего Вашего предприятия).
   Заметьте: БД сервера лицензий будет храниться в папке C:\WINNT\System32\Lserver.
9. Щелкните кнопку Next (Далее).
   Окно Configuring Components (Настройка компонентов) сообщит, что Windows 2000 производит установку и настройку компонентов. Через некоторое время откроется окно Completing the Windows Components Wizard (Завершение работы мастера установки Windows).
10. Щелкните кнопку Finish (Готово).
    Вы снова увидите диалоговое окно Add/Remove Programs.
11. Щелкните кнопку Close (Закрыть) и закройте панель управления.
    Появится сообщение, что для вступления изменений в силу надо перезагрузить компьютер.
12. Щелкните кнопку Yes (Да), чтобы перезагрузить компьютер.
13. Зарегистрируйтесь на Server01 как Administrator (Администратор) с паролем **password.**
14. Раскройте меню Start/Programs/Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Terminal Services Licensing (Лицензирование служб терминалов).
15. Запустится оснастка Terminal Services Licensing (Лицензирование служб терминалов), и откроется окно статуса Terminal Services Licensing Manager (Диспетчер лицензий служб терминалов), которое будет оставаться на экране, пока идет поиск служб терминалов. После обнаружения Server0I появится в правой панели со статусом Not Activated (Не активизирован).
16. В правой панели щелкните SERVER01.
17. В меню Action (Действие) выберите команду Activate Server (Активизировать сервер).
    Запустится мастер лицензирования.
18. Щелкните кнопку Next (Далее).
    Откроется окно выбора способа подключения.
19. В списке Connection Method выберите Telephone и щелкните кнопку Next (Далее).
    Откроется окно выбора страны и региона.
20. Выберите страну и щелкните кнопку Next (Далее).
21. Щелкните кнопку Next (Далее), не вводя идентификационный номер сервера лицензий.
    Появится сообщение, что идентификационный номер сервера лицензий не был введен или введен неправильно.
22. Щелкните кнопку OK.
23. В окне активизации серверной лицензии щелкните кнопку Cancel (Отмена).
24. Закройте оснастку Terminal Services Licensing.

Вы установили компонент Terminal Services Licensing, позволяющий использовать службы Terminal Services в режиме сервера приложений 90 дней. В течение этого срока надо активизировать сервер, используя оснастку Terminal Services Licensing и информацию, предоставленную Вам Microsoft.

► Задание 3: подготовьте приложение к работе на сервере приложений

Удалите средства администрирования Windows 2000, затем переустановите их и убедитесь, что они работают нормально в сеансе связи со службами терминалов. Убедитесь, что установочный компакт-диск Windows 2000 Server вставлен в привод CD-ROM на Server01 и что Вы зарегистрированы на нем как Administrator (Администратор).

1. Раскройте меню Start\Settings (Пуск\Настройка) и щелкните ярлык Control Panel (Панель управления).
2. Дважды щелкните значок Add/Remove Programs.

   Откроется одноименное диалоговое окно.
3. В списке установленных программ выберите Administration Tools (Администрирование Windows 2000) и щелкните кнопку Remove (Удалить).

   Появится запрос, действительно ли Вы хотите удалить средства администрирования Windows 2000 с компьютера.
4. Щелкните кнопку Yes (Да).

   Откроется окно статуса программы установки Windows Installer, а затем — окно статуса Windows 2000 Administration Tools, сообщающее об удалении средств администрирования.

   По завершении удаления посмотрите на диалоговое окно Add/Remove Programs — элемента Windows 2000 Administration Tools там больше нет.
5. Щелкните кнопку Add New Programs (Установка новой программы).
6. Щелкните кнопку CD or Floppy (CD или дискеты).

   Откроется окно Install Program From Floppy Disk or CD-ROM (Установка программы с дискет или компакт-диска).
7. Щелкните кнопку Next (Далее).

   Откроется окно Run Installation Program (Запуск программы установки).
8. В поле Open (Открыть) введите **adminpak.msi**.
9. Щелкните кнопку Next (Далее).

   Запустится мастер установки средств администрирования Windows 2000.
10. Щелкните кнопку Next (Далее).

    Откроется окно Installation Progress (Индикатор установки), отражающее ход установки.
11. По завершении копирования файлов щелкните кнопку Finish.
12. В открывшемся окне щелкните кнопку Next (Далее).
13. Прочитав информацию в следующем окне, щелкните кнопку Finish.

    Вы снова увидите диалоговое окно Add/Remove Programs.
14. Щелкните кнопку Close (Закрыть).
15. Закройте панель управления.

► Задание 4: соединение со службами терминалов в режиме сервера приложений

Установив службы терминалов на Server02, подключитесь с Server02 на Server01. Во время соединения наблюдайте с Server02 за параметрами сеанса при помощи средств, установленных на ServerOl. Зарегистрируйтесь на ServerOl и Server02 в домене MICROSOFT как Administrator.

1. На ServerOl в меню Start (Пуск) выберите команду Run (Выполнить).

   Откроется диалоговое окно Run (Запуск программы).
2. В поле Open (Открыть) введите **C:\winnt\system32\clients** и щелкните кнопку OK.

   Откроется окно Clients.
3. Щелкните папку Tsclient.
4. В меню File (Файл) выберите команду Sharing (Доступ).

   Откроется диалоговое окно Tsclient Properties (Свойства: Tsclient) с выбранной вкладкой Sharing (Доступ).
5. Щелкните переключатель Share This Folder (Открыть обший доступ к этой папке).

   В поле Share Name (Сетевое имя) появится Tsclient.

6. Щелкните кнопку OK.
7. Закройте окно Clients.
8. На Server02 в меню Stan (Пуск) выберите команду Run (Выполнить).

   Откроется диалоговое окно Run (Запуск программы).
9. В поле Open (Открыть) введите **\\server01\tsclient** и щелкните кнопку OK.
10. В открывшемся окне дважды щелкните папку Win32.
11. Дважды шелкните папку disks.
12. Дважды шелкните папку disk1.
13. Дважды щелкните значок setup.

    Откроется окно Terminal Services Client Setup (Установка клиентов служб терминалов).
14. Щелкните кнопку Continue (Продолжить).

    Откроется диалоговое окно Name And Organization Information (Сведения об имени и организации).
15. Введите свое имя и шелкните кнопку OK.

    Откроется информационное окно Confirm Name And Organization Information (Подтверждение сведений о пользователе).
16. Щелкните кнопку OK.

    Откроется информационное окно License Agreement (Лицензионное соглашение).
17. Щелкните кнопку I Agree (Принимаю).

    Откроется диалоговое окно Terminal Services Client Setup (Установка Клиент служб терминалов).

    Заметьте: клиентское ПО установлено в папку Program Files.
18. Щелкните большую кнопку со значком окна для начала установки ПО клиента служб терминалов.

    Откроется диалоговое окно, с запросом, хотите ли Вы предоставить всем пользователям служб терминалов на этом компьютере одинаковые начальные параметры,
19. Щелкните кнопку Yes (Да).
20. В ответ на сообщение об успешной установке щелкните кнопку OK.
21. Закройте окно Disk1.
22. На Server02 раскройте меню Start\Programs\Administrative Tools\ Terminal Services Client (Пуск\Программы\Администрирование\ Клиент служб терминалов) и щелкните ярлык Terminal Services Client (Клиент служб терминалов).

    Откроется диалоговое окно Terminal Services Client (Клиент служб терминалов).
23. В списке Server (Сервер) введите **Server01**.
24. Оставьте параметр Screen area (Область экрана) равным 640x480, убедитесь, что помечен флажок Enable Disk Compression (Включить сжатие данных), и пометьте флажок Cache Bitmaps To Disk (Кэшировать точечные рисунки на диск).
25. Щелкните кнопку Connect (Подключить).

    Откроется окно ServerOl — Terminal Services Client (ServerOl — клиент служб терминалов)
26. В диалоговом окне Log On To Windows (Вход в введите Windows) имя Jane_Doe и пароль **student** и шелкните кнопку OK.

    Обратите внимание на нестандартную цветовую схему. Это свидетельствует о том, что был загружен персональный профиль пользователя Jane_Doe.
27. Не прерывая сеанс связи, раскройте меню Start/Programs/Administrative Tools (Пуск\-Программы\Администрирование) и щелкните ярлык Terminal Services Manager (Диспетчер служб терминалов).

28. В дереве консоли оснастки Terminal Services Manager (Диспетчер служб терминалов) щелкните SERVER01.
29. На правой панели щелкните Jane_Doe.
30. В меню Actions (Действие) выберите команду Status (Состояние).

    Вы увидите информацию о пользовательском сеансе Jane_Doe.
31. Щелкните кнопку Close (Закрыть).
32. В меню Actions (Действие) выберите команду Send Message (Отправить сообщение).

    Откроется диалоговое окно Send Message (Отправка сообщения).
33. В поле заголовка Message title введите **Message from the Administrator** (Сообщение от администратора), а в поле Message — **Terminal** Services **will be shutting down for maintenance in a few minutes. Please close your session** (Через несколько минут службы терминалов завершат свою работу для технического обслуживания. Пожалуйста, закройте Ваш сеанс).
34. Щелкните кнопку OK.

    Пользователь, установивший сеанс связи со службами Terminal Services, увидит сообщение от администратора.
35. Щелкните кнопку OK.
36. Закройте оснастку Terminal Services Manager (Диспетчер служб терминалов), а затем — окно SERVER01 — Terminal Services Client.

    Появится сообщение о завершении сеанса Windows.
37. Прочитайте его и щелкните кнопку OK.
38. Завершите работу Server02 и Server01.

Резюме

Службы Terminal Services, выполняющиеся на Windows 2000 Server, позволяют клиентам выполнять приложения, обрабатывать и хранить данные на сервере. Они предоставляют доступ к рабочему столу сервера при помощи ПО эмуляции терминала. Службы Terminal Services функционируют в режимах удаленного администрирования (Remote Administration) и сервера приложений (Application Server). Первый предоставляет системным администраторам мощный механизм удаленного управления любым компьютером с Windows 2000 Server через любое соединение TCP/IP. Второй обеспечивает централизованное развертывание и управление приложениями, сокращая затраты времени на разработку, развертывание, обслуживание и обновление приложений. Существует четыре компонента лицензирования служб терминалов: Microsoft Clearinghouse, сервер лицензий, сервер терминалов и клиентские лицензии. Развертывание сервера лицензий служб терминалов состоит из следующих этапов: установка сервера лицензий, его включение и активизация и установка лицензий. Минимальные требования, которым должен удовлетворять клиентский компьютер или терминал для соединения с сервером служб Terminal Services, — это возможность установки на нем клиентского ПО и сетевое подключение. Сервер Windows 2000 со службами терминалов, работающими в режиме сервера приложений, поддерживает многопользовательский доступ к любому числу приложений. Развертывание приложений можно производить с помощью Active Directory и оснастки Group Policy, а также с контроллера домена. При установке служб терминалов для Windows 2000 в программную группу Administrative Tools устанавливаются дополнительные средства, в частности Terminal Services Client Creator (Создатель клиента служб терминалов), Terminal Services Manager (Диспетчер служб терминалов), Terminal Services Configuration (Настройка служб терминалов) и Terminal Services Licensing (Лицензирование служб терминалов).

Закрепление материала

? J Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Чем корень DFS отличается от виртуального каталога?

2. Вы открываете документацию по IIS 5.0 из Internet Services Manager (HTML). При этом проблем не возникло. Для доступа к содержащейся в ней информации можно использовать вкладку Index (Указатель). На этой вкладке Вы находите фразу Process Accounting. Однако в результате поиска эта фраза не была найдена. В чем наиболее вероятная причина случившегося?

3. Вы создали виртуальный каталог для WebDAV-публикации. Хотя домашний каталог Web-узла доступен из Internet Explorer 5, доступ к созданному Вами виртуальному каталогу получить не удается. Назовите две причины этой проблемы и возможные пути еерешения.

4. Почему клиент и служба Microsoft Telnet должны поддерживать аутентификацию NTLM?

5. Какие функции при отсутствии лицензий могут выполнять службы терминалов и как долго?

ПРИЛОЖЕНИЕ А

Вопросы и ответы

Глава 1

Закрепление материала

1. Клиент попросил Вас порекомендовать подходящую серверную ОС семейства Windows 2000, исходя из следующих условий:
   - все удаленные офисы соединены со штаб-квартирой предприятия и центром обработки данных высокоскоростными (более 10 Мб/с) каналами;
   - все 10 000 пользователей используют Windows 2000 Professional или Windows98.

   Требования к функциональности:
   - все сайты получат доступ к кластеру высокодоступного сервера с БД Microsoft SQL Server 7.0; двухсерверный кластер с 6 процессорами в каждом компьютере расширять не планируется;
   - остальные серверы будут работать под управлением Windows 2000 с установкой Active Directory, основных файлов, служб печати и удаленного доступа к сети; на них будет установлено 1–4 процессора в зависимости от количества пользователей каждого сайта (например, небольшой удаленный сайт будет работать на однопроцессорном сервере, а на всех серверах корпоративного сайта будет по 4 процессора); на всех этих компьютерах будет установлена одна и та же редакция Windows 2000.
   - каждый домен Active Directory будет поддерживать 2 500 пользователей.

   Windows 2000 Advanced Server рекомендуется устанавливать на кластере SQL Server из двух узлов. Эта ОС поддерживает 2-узловую кластеризацию, 8 процессоров и обеспечивает высокую доступность. Можно установить и Windows 2000 Datacenter, однако данная редакция ОС превышает требования заказчика к кластеризации и многопроцессорной обработке. Windows 2000 Server не удовлетворяет требованиям заказчика для работы SQL Server, так как не поддерживает кластеризацию и 6 процессоров.

   Остальные серверы будут работать под управлением Windows 2000 Server, так как эта редакция ОС отвечает требованиям: поддерживает 4 процессора, Active Directory, удаленный доступ по телефонной линии и службы файлов и печати. Ее легко масштабировать для поддержки 2 500 пользователей на домен и около 10 000 пользователей в сети.
2. Почему WDM-драйверы предпочтительнее старых драйверов Windows NT?

   Драйверы устройств WDM выигрывают от использования общего набора служб ввода-вывода. Поэтому драйверы, разработанные на основе WDM, совместимы на уровне двоичного кода с Windows 2000/98.

Модель WDM основана на структуре класс-минипорт, обеспечивающей модульную расширяемую структуру для поддержки устройств. Это позволяет каждому WDM-классу абстрагировать многие общие детали в управлении схожими устройствами.

3. Как Windows 2000 защищает исполняемые компоненты (Executive) от приложений пользовательского режима?

   Приложения пользовательского режима обращаются к исполняемым компонентам Windows 2000 (Executive), работающим в режиме ядра, через соответствующие подсистемы. Подсистема передает запросы ввода-вывода драйверам режима ядра через службы ввода-вывода. Системные службы доступны как подсистемам пользовательского режима, так и остальным компонентам Executive. Внутренние подпрограммы доступны только компонентам Executive, которые экспортируют подпрограммы, поддерживающие взаимодействие с ядром системы.

4. Какой компонент Executive отвечает за вытесняющую многозадачность?

   Process Manager (Диспетчер процессов) приостанавливает и возобновляет выполнение процессов — это важное свойство любой многозадачной ОС. Process Manager не позволяет процессу монополизировать ресурсы ОС и остановить выполнение остальных процессов.

5. В чем главное отличие рабочей группы от домена?

   Рабочая группа — это распределенный каталог, поддерживаемый на каждом компьютере группы. Домен — централизованный каталог ресурсов, поддерживаемый на контролерах домена и предоставляемый пользователю службами Active Directory.

6. Каковы структура и назначение службы каталогов?

   Служба каталога включает БД, содержащую информацию о сетевых ресурсах (например компьютерах и принтерах), и службы, предоставляющие ее пользователям и приложениям.

Глава 2

Закрепление материала

1. Какую файловую систему выбрать при установке Windows 2000 для двухвариантной загрузки?

   Лучший выбор — FAT. Хотя Windows 2000/NT поддерживают файловую систему NTFS, Windows 2000 использует ряд дополнительных возможностей NTFS 5.0 (например шифрование файлов), которых нет в предыдущих версиях NTFS. Поэтому при запуске Windows NT на компьютере с двумя этими ОС Вы не прочитаете файлы, зашифрованные в Windows 2000.

2. Пользователям в Вашей организации зачастую нужен доступ к нескольким серверам. Какой режим лицензирования следует выбрать и почему?

   Лучший выбор — лицензирование «на рабочее место». Лицензирование каждого клиентского компьютера выгодно, когда большое число клиентских компьютеров обращается к нескольким серверам. Если в описанной ситуации лицензировать серверы, придется для каждого сервера приобрести лицензии на каждый клиентский компьютер в сети.

3. Вы устанавливаете Windows 2000 Server на компьютере, который будет рядовым сервером в имеющемся домене Windows 2000. В ходе установки Вы хотите присоединить компьютер к домену. Какая информация Вам нужна и какие компьютеры должны быть доступны в сети перед запуском программы установки?

   Для присоединения к домену надо знать его DNS-имя. Удостоверьтесь, что учетная запись компьютера для рядового сервера есть в домене. Либо Вы должны иметь право создавать учетные записей компьютеров в этом домене. Сервер, на котором запущена служба DNS, и контролер домена, к которому Вы присоединяетесь, должны быть доступны в сети. Чтобы новый компьютер домена динамически получил IP-адрес, в сети должен быть доступен и DHCP-сервер.

4. Вы устанавливаете Windows 2000 Server с компакт-диска на компьютере, который ранее работал под управлением другой ОС. На жестком диске не хватает места для обеих ОС, и Вы решили заново поделить жесткий диск на разделы и установить Windows 2000 Server на чистый жесткий диск. Опишите два способа деления жесткого диска на разделы.

   Ответ 1. Задействуйте средство разбиения диска на разделы, например утилиту fdisk из MS-DOS, для удаления существующих разделов, создания и форматирования нового раздела. В этот новый раздел и установите Windows 2000.

   Ответ 2. Загрузите компьютер с установочного компакт-диска Windows 2000 Server. **В текстовом режиме установки Вы можете удалить раздел, затем создать и отформатировать новый. Продолжите установку Windows 2000 Server в новый раздел.**

5. Вы устанавливаете Windows 2000 по сети. Какие операции необходимо выполнить на клиентском компьютере перед установкой?

   Узнайте путь к установочным файлам на дистрибутивном сервере. Создайте на целевом компьютере раздел FAT размером 671 Мб (рекомендуется 2 Гб). Создайте дискету с сетевым **клиентом, чтобы затем можно было подключиться к дистрибутивному серверу с компьютера, на котором не установлена ОС.**

6. Вы хотите обновить Windows NT 3.5 Server до Windows 2000. Выберите из списка все возможные способы обновления:

   а) выполнить обновление до Windows NT 3.51 Workstation и затем — до Windows 2000 Server;

   б) выполнить обновление до Windows NT 4.0 Server и затем — до Windows 2000 Server;

   в) сразу выполнить обновление до Windows 2000 Server;

   г) запустить программу Convert.exe, чтобы обеспечить совместимость имеющихся разделов NTFS с Windows 2000, и выполнить обновление до Windows 2000 Server;

   д) выполнить обновление до Windows NT 3.51 Server и затем — до Windows 2000 Server

   Ответ: б и д.

   Ответ а — неправильный, потому что Windows NT **Workstation** (3.5x **или 4.0) нельзя обновить до Windows 2000 Server.**

   Ответ в — неправильный, потому что Windows NT 3.5 **нельзя напрямую обновить до Windows 2000 Server.**

   Ответ г — неправильный, потому что в ходе установки Windows 2000 файловая система NTFS автоматически обновляется до версии 5,0.

7. В Вашей сети ощущается нехватка дискового пространства. Опишите три службы в Windows 2000 Server, которые помогут контролировать и эффективно использовать имеющееся пространство.

   Ответ 1. В NTFS 5.0 для управления дисковым пространством применяются дисковые квоты. Вы можете ограничивать пространство для любого пользователя на любом диске.

   Ответ 2. Сжатие диска позволяет уплотнять данные дисков, каталогов или конкретных файлов. На квоты пользователя сжатие не влияет. Квоты вычисляются на основе размера несжатых файлов.

   Ответ 3. Remote Storage Services **(Службы внешнего хранилища) позволяют освободить место на диске за счет автоматического архивирования редко используемых данных на сменных носителях. Архивированные данные останутся доступными пользователям, хотя их извлечение замедлится.**

Глава 3

Стр. 101

5. Какая папка, отсутствующая в i386, появилась в папке Win2000dist?
   oem

Стр. 101

18. Для чего нужны UDF-файлы?
   UDF-файлы включают уникальные параметры для настройки автоматической установки. Чтобы запустить автоматическую установку, в командной строке надо указать уникальный идентификатор (UniqueID), содержащийся в UDF-файле. При установке файл ответов дополняется уникальными данными и t UDF-файла.

Закрепление материала

1. Для чего применяются ключи /tempdrive: и /t: программ Winnt32.exe или Winnt.exe?
   Ключи /tempdrive: программы Winnt32.exe и /t: программы Winnt.exe копируют установочные файлы Windows 2000 Server на указанное устройство. Например, при выполнении Winn32.exe /tempdrive:d все установочные файлы Windows 2000 копируются на раздел D:. Этот ключ указывает Setup пометить соответствующий раздел как загрузочный.
2. Вам надо разработать стратегию быстрой установки Windows 2000. После оценки условий выделились три категории компьютеров, требующих установки Windows 2000 Server:

- 30 одинаковых компьютеров с Windows NT Server 4.0, которые нужно обновить ло Windows 2000;
- 20 одинаковых компьютеров, на которых надо выполнить новую установку Windows 2000 Server;
- на удаленных сайтах будетвыполнена установка Windows 2000 Server на чистые диски.

Надо обеспечить установку Windows 2000 Server со стандартного образа, соответствующего настройке Вашей локальной ОС. Для этого нужно предоставить жесткие диски для их установки на удаленные серверы.

Перечислите этапы Вашей стратегии установки

Чтобы обновить 30 компьютеров, создайте при помощи Setup Manager (Диспетчер установки) файл ответов и дистрибутивный сетевой ресурс. Используя текстовый редактор, настройте файл ответов. Автоматизировать обновления ОС позволяет продукт типа SMS. Если у Вас нет SMS, запустите Winnt32 с ключом /unattend и другими ключами, предназначенными для автоматизации установки (см. занятие 1).

В случае 20 одинаковых компьютеров установите на один ОС со всеми приложениями, которые надо продублировать на остальные компьютеры. Скопируйте sysprep.exe, sysprepcl.exe и sysprep.inf (в формате файла ответов) в папку $OEM\$1\Sysprep. Убедитесь, что в разделе [GuiRunOnce] файла ответов вызывается программа sysprep.exe с ключом —quiet для продолжения установки без вмешательства пользователя. С помощью утилиты сторонней фирмы создайте образ диска и скопируйте его на каждый из 20 компьютеров. После перезагрузки мастер мини-установки воспользуется данными из файла sysprep.inf.

На удаленных сайтах при подготовке дисков для второй части установки задайте ключ /Syspart. Доставьте жесткий диск с образом на удаленный сайт; тамошние администраторы должны установить эти диски в свои серверы как загрузочное устройство. Если используется SCSI-аппаратура, диск с образом должен иметь номер 0 или 7.

Можно задействовать и загрузочный компакт-диск. При этом для автоматизации установки нужна дискета с файлом winnt.sif.

3. Для чего Setup Manager (Диспетчер установки) создает папку OEM и ее подпапки?

   Папка oem содержит необязательный файл cmdlines.txt, подпапки файлов изготовителей оборудования и файлы, необходимые для завершения или настройки автоматической установки. Подпапки oem содержат все файлы, не включенные в стандартную установку Windows 2000 Server. Эти подпапки проецируются на конкретные разделы и каталоги компьютера, на котором выполняется автоматическая установка. Ниже поясняется назначение каждой подпапки SoemS.

   $$ — копируются файлы из дистрибутивной папки в $windir$ или $systemroot$. Для стандартной установки Windows 2000 Server эти переменные указывают на C:\Winnt, как и другие подпапки в ней, например Help для справочных файлов и System32 для файлов, которые надо копировать в каталог System32.

   $1 — копируются файлы из дистрибутивной папки в корневой каталог системного диска. Ее расположение совпадает со значением переменной %systemdrive%. В типичной установке Windows 2000 Server эта переменная указывает на корневой каталог устройства C:\. Папка $1 содержит подпапки для установки драйверов сторонних фирм.

   Буква диска — папки, получающие имя после привязки конкретной буквы диска к букве диска на локальном компьютера. Например, если при установке надо скопировать файлы на диск E:, создайте папку E и разместите в ней нужные файлы и папки.

   Textmode — содержит специальные HAL и драйверы накопителей, необходимые для установки и запуска Windows 2000 Server.

4. Чем отличается установка с помощью файла Cmdlines.txt от установки с помощью раздела [GuiRunOnce] файла ответов?

   Команды из файла Cmdlines.txt выполняются в контексте учетной записи до входа пользователя в систему. В этот файл включаются любые команды, которые можно выполнить без входа пользователя в систему. Команды из раздела [GuiRunOnce] выполняются в контексте учетной записи после первого входа пользователя в систему. Это идеальный способ запуска сценариев для конкретных пользователей, например добавления принтеров или автоматической настройки электронной почты.

5. Чем отличаются утилиты Syspart и Sysprep?

   Syspart — ключ программы Winnt32.exe. Он завершает предварительное копирование в ходе установки Windows 2000 Server. После этого жесткий диск со скопированными файлами можно установить на другой компьютер. После загрузки с этого диска продолжится текстовая фаза установки. Syspart идеально подходит для ускорения установки на различающихся системах. Установку с помощью Syspart можно автоматизировать, включив файл ответов, а также используя Syspart из командной строки Winnt32.

   Sysprep готовит компьютер к созданию образа диска после установки ОС и приложений. Образ, созданный соответствующей утилитой, можно скопировать на одинаковые или похожие компьютеры. Установку на них продолжит мастер мини-установки. Дополнительно **автоматизировать его работу позволяет файл** Sysprep.inf.

Глава 4

Закрепление материала

1. Как установить новый жесткий диск объемом 10 Гб, который надо разбить на 5 секций по 2 Гб каждая?

   Можно оставить диск в базовой конфигурации и создать на нем комбинацию из основных разделов (до 3) и логических дисков в дополнительном разделе или обновить диск до динамического, а затем создать 5 простых томов, каждый по 2 Гб.

2. Вы хотите создать чередующийся том на компьютере с Windows 2000 Server. У Вас хватает неразмеченного пространства на двух дисках, но в контекстном меню для свободного места доступна только команда создания нового раздела. В чем проблема и как ее решить?

   Чередующиеся тома можно создать только на динамических дисках, разделы — только на базовых, а тома — только на динамических. Перед созданием чередующегося тома надо обновить все диски в будущем томе до динамических.

3. Ваш компьютер способен загружать Windows 98 и Windows 2000. Вы преобразовали один из дисков с архивными файлами из базового в динамический. После этого из Windows 98 прочесть файл с этого диска стало невозможно. В чем причина?

   Читать **динамическое хранилище может только Windows 2000.**

4. Какие разрешения назначаются по умолчанию при форматировании раздела под NTFS? Кто сможет получить доступ к этому разделу?

   Группе Everyone (Все) предоставлено разрешение Full Control (Полный доступ). Все пользователи являются членами этой группы, поэтому все они получат доступ.

   Разрешение по умолчанию — **Full Control. Группа Everyone имеет полный доступ к тому.**

5. Назовите эффективные разрешения пользователя, если ему предоставлено разрешение Write, а его группе — Read для одной и той же папки.

   Пользователь вправе читать и записывать в папку, потому что разрешения NTFS суммируются.

6. Что происходит с разрешениями файла при его перемещении из одной папки в другую в рамках одного раздела NTFS? Что происходит при перемещении файла на другой раздел NTFS?

   При перемещении файла из одной папки в другую в пределах одного раздела NTFS файл сохраняет свои разрешения. При перемещении в папку другого раздела NTFS **файл** наследует **разрешения целевой папки.**

7. Как сменить владельца файлов и папок увольняющегося сотрудника?

   Чтобы завладеть папками и файлами сотрудников, надо иметь полномочия администратора. Чтобы позволить работнику завладеть **папками и файлами, предоставьте ему специальное разрешение доступа Take Ownership (Смена владельца).**

8. Назовите лучший способ обеспечить безопасность общих ресурсов на разделе NTFS.

   Поместите файлы, к которым Вы хотите открыть доступ, в общую папку и оставьте у нее разрешения по умолчанию — группа Everyone (Все) с разрешением Full Control (Полный доступ). Назначьте пользователям и группам разрешения NTFS **для доступа ко всему содержимому общей папки или для доступа к конкретным файлам.**

Глава 5

Стр. 199

9. Какая из папок ссылается на ресурс вне Server01?

   Физический путь к папке intranet на **Server02 — C:\inetput\wwwroot.**

Стр. 199

10. Какая из папок ссылается на диск, подключенный к ранее пустому каталогу?

    Палка ftp была до этого пустой папкой на ServerOl. Путь к пустой папке — C:\inetput\ftproot. Этот каталог указывает на дополнительный раздел диска 0.

Стр. 199

11. Выполняя данное упражнение, Вы создали реплику DFS-ссылки Press. Имя реплики – \\SERVER01\PressRepl. DFS-ссылка представляет общую папку PressRepl и находится в каталоге C:\Public\Press. Просмотрев содержимое данного каталога, Вы обнаружите, что он пуст. Однако, если просмотреть DFS-ссылку News, Вы увидите в соответствующей папке файл Press.wri. Почему DFS-реплика PressRep! пуста?

Потому что репликация и синхронизация не поддерживаются для изолированных DFS. Надо вручную колировать все файлы, появляющиеся в H:\Press (сетевой ресурс \\Server01\Press) в каталог C:\Public\Press (сетевой ресурс \\Server01\PressRepl), чтобы \\Server01\ PressRepl служил репликой \\Server01\Press. После копирования DFS-ссылка \\Server01\Public\News будет отказоустойчивой — в случае недоступности \\Server01\ Press пользователи смогут обратиться к \\Server01\\PressRepl.

Закрепление материала

1. Чем корень DFS отличается от диска, подключенного к пустой папке?

Смонтированный к пустой папке диск позволяет перенаправить папки. При сохранении файлов в папку, указывающую на смонтированный раздел, файлы перенаправляются на этот раздел. Корень DFS предоставляет центральную точку, в которой разрозненные ресурсы связываются DFS-ссылками. Эти ссылки представляются пользователям как единый сетевой ресурс, содержащий подпапки. В результате достигается ограниченное объединение ресурсов.

2. Выполняя упражнения, Вы заметили, что команды New Root Replica (Создать корневую реплику) и Replication Policy (Политика репликации) в оснастке Distirbuted File System были недоступны. Почему?

Команды New Root Replica (Создать корневую реплику) и Replication Policy (Полшика репликации) доступны только для доменных корней DFS. В упражнении 1 Вы настраивали изолированный корень DFS. Корневая реплика позволяет тиражировать корень DFS на другие серверы сети. Это обеспечивает отказоустойчивость и равномерную загрузку сети. При отказе сервера с корнем DFS пользователи смогут обратиться к его репликам на других серверах. Если доступны все серверы с репликами корней DFS, они обеспечивают равномерную загрузку сети при выполнении запросов пользователей. Политика репликации позволяет задать параметры тиражирования корней DFS и сетевых ресурсов в их составе.

3. Почему DFS не предоставляет собственной системы защиты?

Безопасность обеспечивается основной файловой системой. DFS-ссылки, указывающие на NTFS-разделы, используют разрешения NTFS или разрешения для сетевого ресурса. На разделах FAT доступ ограничивается только к сетевым ресурсам. При доступе к ресурсам DFS на разделах с другими ОС применяются назначенные в этих ОС права и разрешения. Открыть доступ к ресурсам NetWare посредством DFS позволяют службы Gateway Services for NetWare (Службы шлюза для NetWare).

4. Объясните роль процесса проверки согласованности знаний (KCC) в синхронизации хранилища Active Directory между контроллерами домена?

Для репликации внутри домена KCC применяет кольцевую топологию. Она указывает путь для обновлений хранилищ Active Directory между контролерами домена и предоставляет пути для надежной репликации с каждой стороны кольца на тот случай, если кольцевая структура временно нарушена.

5. Какие данные реплицирует служба FRS?

Данные системного тома, а также корней и ссылок DFS.

Глава 6

Стр. 244

3. Проверьте каждый из контейнеров, входящих в microsoft.com. Не меняйте информацию в этих контейнерах.

   Что представляют собой пункты ниже microsoft.com и каково их назначение? Подсказка: изучите свойства каждого контейнера в дереве консоли, чтобы узнать об их назначении.

   Built-in содержит локальные группы, созданные при установке контроллера домена.

   Computers **— контейнер по умолчанию для обновленных учетных** записей **компьютеров. Если требуется, можно переместить эти компьютеры в другие контейнеры.**

   Domain Controllers **— контейнер по умолчанию для новых контроллеров домена** Windows 2000. В этом **контейнере находится Server01.**

   Foreign SecurityPrincipals — контейнер по умолчанию для идентификаторов безопасности (SID) объектов из внешних доверяемых доменов.

   Users **— контейнер по умолчанию для обновленных и встроенных учетных записей пользователей.**

Стр. 245

4. Изучите информацию в его первом окне и щелкните кнопку Next (Далее).

   Управляет доверительными отношениями между доменами.

   Управляет пользователями, компьютерами, группами безопасности и другими объектами в **Active Directory.**

   Создает сайты для управления репликацией **информации Active Directory.**

   DNS управляет службой доменных имен (DNS), преобразующей DNS-имена **компьютеров в IP-адреса.**

Закрепление материала

1. Каково назначение файла Ntdis.dit?

   В файле NTDIS.DIT содержится хранилище Active Directory.

2. Опишите требование для размещения SYSVOL.

   Папка SYSVOL должна находится на разделе NTFS 5.0.

3. Каково назначение SYSVOL? Назовите единственное требование для размещения SYSVOL на диске.

   В папке SYSVOL находится копия доступных доменных файлов контролеров домена. Содержимое этого каталога дублируется на все контролеры домена.

4. В чем разница между атрибутом и значением атрибута? Приведите примеры.

   Атрибуты (или свойства) являются категориями информации и задают характеристики всех объектов определенного типа. Объекты одного типа имеют одинаковые атрибуты. Значения этих атрибутов делают объекты уникальными. Например, все объекты учетных записей пользователей имеют атрибут First Name (Имя), но значением этих атрибутов может быть любое имя, скажем, Алексей или Максим.

5. В чем разница между изменением объекта и изменением атрибута экземпляра объекта?

   Изменение объектов **выполняется из оснастки** Schema **Manager (Диспетчер схемы) (Schmmgmt.msc). Изменение атрибутов экземпляра** объекта **приводит к изменениям** данных, **хранящихся в объекте.**

6. Нало разрешить менеджеру отдела продаж создавать, изменять и удалять учетные записи сотрудников его отдела. Как это сделать?

   Поместите все учетные **записи пользователей из** отдела продаж в **ОП и предоставьте право управления последним руководителю** отдела продаж.

7. Что такое глобальный каталог и каково его назначение?

   Глобальный **каталог хранит ключевую информацию о каждом объекте** дерева домети **или леса, а также частичную реплику всего каталога. Так как в глобальном** каталоге **хранится наиболее** важная **информация об объектах, его репликация** эффективнее, **чем дублирование** всего **хранилища Active Directory.** Глобальный каталог **позволяет пользователям вести** поиск **информации независимо от ее размещения в конкретном домене** дерева **или леса.**

Глава 7

Стр. 276

6. В каком режиме работает консоль?

   Консоль **работает в авторском режиме, как** показано в **списке Console Mode (Режим консоли).**

Стр. **289**

13. Когда окончится срок действия данной учетной записи?

   Согласно текущим параметрам в области Account Expires (Окончание срока **действия учетной записи)** вкладки **Account (Учетная запись)** учетная **запись** имеет **неограниченный срок** действия.

Стр. 290

5. Закройте окно сообщения, щелкнув кнопку OK.

   Вошли ли Вы в систему? Почему?

   Вы не смогли войти в систему локально, **поскольку это разрешение не предоставлено обычным учетным записям пользователей. По умолчанию локально входить в систему на контролере** домена **имеет право его администратор.**

Закрепление материала

1. Можно ли добавить к стандартным консолям Windows 2000 Server оснастки? Почему?

   Добавлять оснастки в стандартные консоли MMC из программной группы Administrative Tools нельзя. Эти консоли настроены для работы в пользовательском режиме. Их можно открыть в авторском режиме, указав ключ/а команды **MMC и путь к MSC-файлу:**

   ```
   mmc /a %SystemRoot%\system32\compmgmt.msc /s
   ```

   В результате консоль Computer Management (Управление компьютером) откроется в авторском режиме.

2. Пользователи жалуются на окно, появляющееся каждый раз, когда они входят в систему. В меню Startup (Автозагрузка) ярлыков нет. После закрытия окна, выхода из системы и перезагрузки компьютера, окно по-прежнему появляется при входе в систему. Какова наиболее вероятная причина этой проблемы и как ее устранить?

   Всем этим **пользователям** назначен **обязательный сетевой профиль. После создания шаблона профиля окно было** остановлено **открытым на рабочем столе. Для решения этой** проблемы убедитесь, **что никто не использует профиль, и переименуйте** файл **Ntuser.man в Ntuser.dat,** чтобы **он перестал быть обязательным. Войдите в систему по учетной записи, использующей этот профиль, закройте открывшееся окно и, завершив сеанс,** выйдите из

системы. По завершении сеанса изменения сохранятся в сетевой папке профилей. Переименуйте соответствующий файл Ntuser.dat в Ntuser.man и сообщите пользователям о возможности повторного входа в систему.

3. В каких случаях использовать группы безопасности вместо групп распространения?

   Для назначения разрешений используйте группы безопасности. Группы распространения применяйте для решения проблем, не связанных с безопасностью, скажем, для распространения списка адресов электронной почты. Для назначения разрешений группы распространения использовать нельзя.

4. Каковы последствия изменения режима домена со смешанного на основной?

   Контролеры домена пред-Windows 2000 не могут быть участниками домена основного режима.

   Изолированные серверы пред-Windows 2000 и компьютеры с Windows NT Workstation могут быть участниками домена.

   После перехода в основной режим вернуться в смешанный нельзя.

5. В каком порядке групповая политика реализована в иерархии хранилища Active Directoryпоумолчанию?

   Групповая политика реализуется в следующем порядке: сайт, домен и затем ОП.

   Для управления наследованием политики группы служит флажок Block Policy Inheritance (Блокировать наследование политики). Впрочем, назначение параметра No Override (Не перекрывать) на более высоких уровнях иерархии переопределяет этот параметр. Кроме того, можно ограничивать область применения групповой политики, изменив параметры безопасности политики.

6. Что такое GPO, GPC и GPT?

   GPO — объект групповой политики. GPO содержит параметры группой политики. Их настраивают для доступа к сайтам, доменам или ОП. GPO хранит информацию о групповой политике в двух местах: GPC и GPT.

   Контейнер групповой политики GPC является объектом Active Directory, содержит свойства GPO и включает подконтейнеры с политиками для компьютеров и пользователей. GPC содержит хранилище классов для распространения приложений. Хранилище классов Windows 2000 представляет собой серверный репозитарий правил для всех приложений, интерфейсов и API, обеспечивающих публикацию и назначение приложений.

   Шаблон групповой политики GPT представляет собой структуру папок в папке системного тома (Sysvol) контроллера домена. GPT — контейнер для всей программной политики, правил распространения сценариев, файлов, приложений и информации о параметрах безопасности. Имя папки, где хранится GPT, является глобальным уникальным идентификатором (GUID) созданного Вами GPO.

Глава 8

Закрепление материала

1. В чем разница между устройством печати и принтером?

   Устройство печати — аппаратура, печатающая страницы или создающая файл на диске (при печати в файл), который затем можно направить на принтер. Принтер — программный интерфейс для одного или нескольких устройств печати,

2. Ваш коллега запретил Вам удалять системную группу Everyone (Все) из разрешений принтера, иначе, по его словам, никто не сможет управлять принтером и его очередью. В чем он не прав? Как можно избежать подобной проблемы?

После удаления из списка разрешений принтера системной группы Everyone (Все) в нем останутся группы Administrators (Администраторы), Creator Owner (Создатель-владелец), Printer Operators (Операторы печати) и Server Operators (Операторы сервера), по умолчанию имеющие доступ к принтеру. Удаление системной группы Everyone (Все) не то же самое, что явный запрет доступа к принтеру для этой группы. В последнем случае управлять принтером будет нельзя, пока пользователь с правами Creator Owner не снимет запрет.

3. В Вашей сети два сервера печати. При подключении пользователя с Windows 95 к одному из них печать выполняется автоматически. Когда тот же пользователь подключается к этому же серверу печати, но к другому принтеру, то получает сообщение о необходимости установить драйвер. В чем причина?

   Для одного из этих принтеров были установлены дополнительные драйверы печати для Windows 95/98, а для другого — нет.

4. Многие сотрудники Вашей организации используют одно устройство печати. Как избежать путаницы пользователей в документах?

   Для идентификации и отделения напечатанных документов создайте страницу-разделитель.

5. Можно ли перенаправить на другой принтер отдельный документ?

   Нет. Вы можете только перенастроить сервер печати, чтобы посылать документы на другой принтер или устройство печати; в итоге все документы будут перенаправляться на этот принтер. Печатаемые и поставленные в очередь документы перенаправить нельзя.

6. Пользователю нужно напечатать очень большой документ. Как это сделать в нерабочее время, не присутствуя при печати?

   Можно указать время печати документа на вкладке General (Общие) диалогового окна свойств задания печати. Чтобы открыть это окно, дважды щелкните значок принтера в окне Printers (Принтеры), в открывшемся окне щелкните документ и выберите в меню Document (Документ) команду Properties (Свойства). Щелкните переключатель Only From (только с) в области Schedule (Расписание) и задайте время, в которое начнется печать документа. Задайте время To (по) за пару часов до начала работы. Чтобы задать время печати, необходимо быть владельцем документа или иметь разрешение управлять документами для соответствующего принтера.

Глава 9

Закрепление материала

1. Ваш компьютер получает конфигурационные сведения TCP/IP от сервера DHCP. Получив эти сведения, Вы можете подключиться к любому узлу своей подсети, а связаться или опросить какой-нибудь узел в удаленной подсети — нет. Вы проверили службу DHCP и убедились, что для Вашей области адресов указана корректная информация о маршрутизаторе. В чем вероятная причина проблемы и как ее устранить?

   На Вашем компьютере неправильно задан шлюз по умолчанию. Параметры шлюза, указанные на клиентском компьютере, имеют более высокий приоритет, чем полученные от сервера DHCP. Для решения проблемы просто удалите информацию о шлюзе по умолчанию с клиентского компьютера и запустите из командной строки утилиту ipconfig с ключом /renew. Другая возможная причина в том, что шлюз по умолчанию недоступен или неверно задана маска подсети.

2. Установив NWLink IPX/SPX и GSNW, Вы не можете связаться с одним из серверов NetWare. При подключении к этому серверу с клиента Windows 2000 Professional, на котором установлены протокол NWLink IPX/SPX и служба CSNW, проблем не во [ни-

кает. Вам надо обеспечить взаимодействие Windows 2000 Server с этим сервером NetWare, поскольку последний содержит ресурсы, которые Вам надо предоставить пользователям с сетевым клиентом Microsoft. В чем вероятная причина проблемы?

Реализация NWLink в Windows 2000 способна **автоматически определить** кадр только **одного типа для IPX/SPX-совместимых протоколов. Так что Windows 2000 Server** может **и неверно распознать тип кадра. Если в сети применяются кадры разных типов, задайте тип кадра сервера NetWare вручную.**

3. Вы заметили, что доступ к сетевым ресурсам с Вашего компьютера Windows 2000 Server осуществляется медленнее, чем с других идентичных компьютеров Windows 2000 Server той же сети. Единственное отличие, которое Вы обнаружили — на «медленном» компьютере установлено несколько протоколов. Как решить эту проблему, используя порядок привязки протоколов?

   Порядок привязки позволяет **оптимизировать производительность сети,** если на компьютере **установлено несколько протоколов, например NetBEUI, NWLink IPX/SPX и TCP/IP. Поскольку большинство серверов** сети **используют только TCP/IP, привязка службы Workstation (Рабочая станция) к TCP/IP должна быть в списке привязок этой службы первой. Тогда при подключении к компьютеру Workstation сначала** попытается **задействовать протокол TCP/IP.**

4. Когда клиенты DHCP пытаются продлить аренду IP-адреса?

   По истечении половины времени аренды клиенты DHCP пытаются обновить первоначально полученные адреса с сервера DHCP. Если попытка обновления неудачна, клиент DHCP предпримет следующую по истечении трех четвертей времени аренды адреса.

5. Для чего может потребоваться определить на сервере DHCP несколько областей?

   Для централизации администрирования и назначения конкретных IP-адресов для подсети **(например** шлюза **по умолчанию)** на сервере **DHCP можно создать несколько** областей. **Для конкретной подсети можно задать** только **одну** область,

6. Как вручную восстановить БД DHCP?

   Откройте раздел реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters, задайте параметру RestoreFlag значение 1 и перезапустите службу DHCP. Второй способ — скопировать резервную копию папки DHCP в каталог DHCP и перезапустить **эту службу,**

7. Перечислите конфигурационные требования для установки сервера WINS.

   Нужен компьютер Windows 2000 Server с настроенными службой WINS, статическим IP-адресом, маской **подсети и шлюзом по умолчанию.**

   На сервере WINS можно также настроить статическую привязку для всех *не-WINS-клиентов*, включить поддержку WINS на сервере DHCP и установить прокси-агент WINS на WINS-клиенты.

8. Зачем может потребоваться несколько серверов имен?

   Установка нескольких серверов имен обеспечивает избыточность, снижает нагрузку на серверы, где **хранится** файл **БД главной зоны, и ускоряет удаленный доступ.**

9. Для чего создаются зоны прямого и обратного просмотра?

   Сервер имен должен иметь **минимум одну зону прямого поиска, отвечающую** за разрешение **имен.**

   Обратная зона поиска необходима для утилит диагностики, например nslookup, и для записи в журналы IIS имен вместо IP-адресов.

10. В чем разница между DNS и Dynamic DNS?

    Динамическая DNS позволяет автоматически обновлять файл зоны первичного сервера. В обычной DNS приходится вручную обновлять файл зоны при добавлении новых хостов или доменов.

Динамическая DNS также позволяет инициировать обновления нескольким авторизованным серверам. Список таких серверов может включать вторичные серверы имен, контроллеры доменов и другие серверы, регистрирующие клиентов в сети, например, серверы WINS и DHCP.

Глава 10

Закрепление материала

1. Поясните назначение маршрутизации вызова по требованию.

   Маршрутизация вызова по требованию обеспечивает связь между удаленными маршрутизаторами. Это позволяет двум маршрутизаторам отдельных сетей использовать коммутируемые телефонные сети или Интернет для связи и передачи информации. Двустороннее соединение позволяет каждому маршрутизатору принимать входящие данные и отправлять исходящие.

2. Какие поставщики служб проверки подлинности существуют в RRAS и чем они отличаются от методов аутентификации?

   Поставщиков проверки подлинности два: Windows и RADIUS. Windows аутентифицирует пользователей с помощью каталога Windows 2000. RADIUS для этого применяет сервер Microsoft IAS RADIUS или сервер RADIUS сторонней фирмы. Метод аутентификации — это процесс согласования клиентом и сервером процедуры аутентификации учетных записей. RRAS поддерживает методы EAP, MS-CHAP 2, MS-CHAP, CHAP, SPAP, PAP и аутентификацию открытым текстом.

3. Каково назначение VPN и какие две технологии VPN поддерживает RRAS в Windows 2000?

   VPN обеспечивает безопасную передачу данных по общедоступным сетям. Windows 2000 RRAS поддерживает две технологии VPN: PPTP и L2TP.

4. Клиент удаленного доступа начинает подключаться к серверу RRAS, но соединение прерывается. Как устранить эту ошибку?

   1) Убедитесь, что включена регистрация событий и просмотрите системный журнал на компьютере с RRAS.

   2) На удаленном клиенте откройте окно свойств устройства удаленного доступа, например модема. Перейдите на вкладку Diagnostics (Диагностика) и пометьте флажок Record a Log (Вести журнал). После следующей попытки соединения просмотрите журнал соединения.

   3) На сервере откройте диалоговое окно Authentication Methods (Методы проверки подлинности) и пометьте флажок Allow remote systems to connect without authentication (Разрешить подключение удаленных систем без проверки). Затем попытайтесь вновь установить соединение с клиентского компьютера.

5. В чем сходство разрешения удаленного доступа Deny Access (Запретить доступ) (в смешанном или основном режиме) с политикой удаленного доступа по умолчанию в домене основного режима?

   Разрешение Deny Access (Запретить доступ) не позволит пользователю подключаться к серверу удаленного доступа. Для доменов основного режима по умолчанию задана политика Deny Remote Access Permission At All Times, а смешанного — Allow Access If Dial-In Permission Is Enabled.

6. Вам надо сконфигурировать 10 серверов RRAS для клиента. Все будут иметь одинаковые конфигурации RRAS. Как наиболее эффективно выполнить эту задачу?

   Настройте один сервер RRAS как мастер конфигурации для остальных серверов RRAS. Скопируйте базовую конфигурацию командой netsh с параметром –c и импортируйте ее на

остальные RRAS-серверы командой netsh *с* **параметром** -f. **Например, для копирования конфигурации** сервера RRAS1 **в** файл сценария Ras.scr **наберите на** RRAS1:

```
netsh -c RAS dump > ras.scr
```

Затем для применения этой политики на сервере RRAS2 наберите на RRAS1:

```
netsh -r RRAS2 -f ras.scr
```

Глава 11

Закрепление материала

1. Какой ключ предназначен для создания цифровых подписей — открытый или закрытый? Объясните ответ.

   Закрытые ключи связаны с созданием цифровых подписей и позволяют изменить данные так, чтобы пользователи были полностью уверены **в Вашем авторстве зашифрованной информации.** Расшифровка **данных осуществляется** с **помощью открытых ключей. Для** создания **цифровой** подписи **применяются только закрытые ключи.**

2. Какие способы удостоверения личности могут быть использованы, если в Вашей сети компьютеры клиентов с Windows 2000 и Windows NT обращаются за аутентификацией на серверы Windows 2000 Server и Windows NT Server?

   Клиентские компьютеры Windows NT могут аутентифицироваться как Windows 2000-, так и Windows NT-серверами **посредством реквизитов NTLM. Для этого они** должны предоставить имя **домена Windows NT, имя пользователя и зашифрованный пароль.** Клиентские **Windows 2000-компьютеры могут** аутентифицироваться **на компьютерах с Windows** 2000 **Server по протоколу Kerberos. Для** этого **они должны предоставить имена домена и пользователя и пароль, зашифрованный к формате** Kerberos. **Windows 2000-компьютеры также могут аутентифицироваться на компьютерах с Windows NT Server посредством NTLM.**

3. Как с помощью шаблона безопасности упростить настройку и анализ параметров безопасности?

   Шаблон можно применить к БД конфигурации безопасности, созданной в оснастке Security Analysis **and Configuration (Анализ и настройка безопасности). После создания базы данных текущие параметры компьютера сравниваются с параметрами политики. Выявив различия, Вы можете использовать** эту оснастку **для согласования параметров безопасности компьютера и шаблона.**

4. Как открыть Web-страницу для работы с сертификатами и для чего она предназначена?

   Web-страница **работы с сертификатами** позволяет **легко создавать и просматривать запросы сертификатов, а также искать CRL и сертификаты.**

5. Какие действия Вы должны предпринять для аудита определенных объектов на контроллерах домена, в котором активна групповая политика?

   Открыть **групповую политику** (как **правило, стандартный GPO** домена или контролера домена) **можно из оснастки** Active **Directory Users And Computers (Active Directory – пользователи и компьютеры). Раскройте узел Windows Settings\Security Settings\Local Policies**Audit **Policy (Конфигурация Windows\Параметры безопасности\Локальные политики\-** Политика **аудита). В правой панели дважды щелкните Audit Object** Access **(Аудит доступа к объектам) и настройте аудит успешных или неудачных попыток доступа. В Windows Explorer (Проводник) найдите конкретные файлы и папки, к которым Вы хотите получить** доступ. **Откройте окно свойств** файла **или папки, перейдите на вкладку Security (Безопасность) и щелкните кнопку Advanced (Дополнительно). В диалоговом окне** Access **Control** Settings (Параметры управления доступом) **щелкните кнопку** View/Edit **(Показать/изме-**

нить). Измените политику аудита для выбранного пользователя или группы или включите аудит для нового пользователя или группы. Не ведите аудит большого числа объектов файлов, поскольку это повышает нагрузку на процессор.

Глава 12

Закрепление материала

1. На Вашем компьютере по умолчанию загружается Windows 2000 Server, но можно загрузить и Windows NT 4.0. После изменения атрибутов файлов в %systemdrive% и удаления некоторых из них компьютер перестал выполнять двухвариантную загрузку. Windows 2000 загружается нормально. Проблема появилась после того, как Вы удалили файл. Как называется этот файл и как исправить эту ошибку?

   Вы удалили файл Boot.ini, необходимый для альтернативной загрузки нескольких ОС. Если его нет, загружается ОС по умолчанию. Для восстановления этого файла запустите ERD, выберите Manual Repair (Ручное восстановление) и затем — Inspect Startup Environment (Анализ среды загрузки).

2. Для своего мобильного компьютера Вы создали три профиля оборудования: Docked (Пристыкован), Undocked On The Network (Отстыкован в сети) и Undocked At Home (Отстыкован дома). После перезагрузки первые два профиля остались, а третий исчез. Назовите наиболее вероятную причину отсутствия профиля Undocked At Home.

   В свойствах профиля Undocked At Home не помечен флажок Always Include This Profile As An Option When Windows Starts (Всегда выводить этот профиль как вариант при загрузке Windows).

3. Почему недоступен флажок Use Hardware Compression. If Available (Использовать аппаратное сжатие, если возможно) в мастере Backup?

   Этот параметр доступен, только если установлен накопитель на магнитной ленте, поддерживающий аппаратное сжатие.

4. Вы создали полную резервную копию в понедельник. В оставшиеся дни недели Вы хотите копировать только те файлы и папки, которые изменялись за прошедший день. Какой тип архива выбрать?

   Добавочный. В такой архив копируются файлы с архивными атрибутами, установленными с момента последнего архивирования, после чего атрибуты архива сбрасываются. Поэтому со вторника по пятницу будут архивироваться только изменения, внесенные за прошедший день.

5. Как проверить настройку службы UPS?

   Отказ питания можно сымитировать, отсоединив шнур питания от ИБП. Во время тестирования подсоединенные к ИБП компьютер и периферия должны работать, а система, сообщив об отказе питания — продолжить регистрацию событий.

   Вы также можете дождаться предельного уровня разряда батарей ИБП, чтобы проверить корректное завершение работы системы. Восстановите питание ИБП и проверьте журнал событий — в нем должны быть отражены все действия и отсутствовать ошибки.

   Данная процедура требует подключения ИБП к компьютеру через COM-порт или специальный интерфейс, поставляемый с ИБП.

Глава 13

Закрепление материала

1. Вы воспользовались утилитой Compact для сжатия файлов подпапки Users на разделе NTFS и пометили флажок Display Compressed Files And Folders With Alternate Color (Отображать сжатые файлы и папки другим цветом). Через неделю Вы решили при помощи Windows Explorer проверить, сжаты ли файлы. Вложенные папки учетных записей пользователей в каталоге Users, созданные после запуска утилиты Compact, оказались несжатыми. **Почему** это произошло и как решить проблему?

   Вы запустили утилиту **Compact и сжали все вложенные папки Users. В итоге все подпапки, кроме родительской папки Users, были помечены для сжатия. Поэтому новые папки, созданные в папке Users, не** сжимаются. **Решить данную проблему можно несколькими способами. Например, пометить для сжатия палку Users и все** ее **подпапки утилитой** compact: **перейдите на диск с родительской папкой Users и в командной строке наберите compact /s:Users** /c. **Или: сжав подпапку Users с** помощью **проводника Windows, выберите переключатель Apply changes to** this **folder, subfolders** and **files (К этой папке и ко всем вложенным** папкам **и файлам).**

2. Ваш отдел недавно заархивировал несколько гигабайт данных с компьютеров Windows 2000 Server на компакт-диски. После тою, как пользователи добавили файлы на сервер, Вы заметили, что время доступа к жесткому диску увеличилось. Как ускорить доступ к диску сервера?

   Дефрагментируйте файлы на жестком диске сервера посредством утилиты Disk Defragmenter (Дефрагментация диска).

3. Вы администратор компьютера Windows 2000 Server, на котором хранятся домашние каталоги и перемешаемые профили пользователей. Вам требуется ограничить размер каждого домашнего каталога до 25 Мб и одновременно осуществлять мониторинг, но не ограничивать объем дискового пространства, используемый для хранения перемещаемых профилей. Как настроить тома на сервере?

   Создайте два тома: для хранения домашних папок и для хранения перемещаемых пользовательских профилен. Для домашней папки укажите максимальный размер *25* **Мб и** пометьте **флажок Deny Disk** Space **To Users Exceeding Quota Limit. Для** тома **перемещаемых профилей не** задавайте квоту **и сбросьте вышеуказанный** флажок.

4. Производительность сервера снизилась. Вам требуется получить суммарную информацию по производительности сервера, и Вы хотите воспользоваться утилитой, которая предоставит подробные сведения об узких местах системы. Что сделать для мониторинга работы сервера по мере роста количества подключенных к нему пользователей после решения проблемы производительности?

   Чтобы получить сводку производительности сервера, запустите Task Manager (Диспетчер задач) и понаблюдайте за **изменением параметров на вкладке** Performance **(Производительность). Это поможет выявить узкие места системы.** Затем **запустите оснастку** System Monitor **(Системный монитор) и просмотрите значения** счетчиков **производительности. При необходимости** добавьте **ресурсы** или удалите **приложения — источники узких мест. Устранив проблемы, запустите оснастку Performance Logs And** Alerts **(Оповешения и журналы производительности) для протоколирования параметров производительности. Полученные** журналы **послужат отправной точкой для анализа производительности. Если Вам кажется, что причина снижения производительности** в сетевой **активности, проанализируйте** трафик **через Network Monitor (Сетевой монитор).**

5. Вам требуется отфильтровать весь сетевой трафик и выделить трафик между двумя компьютерами; кроме того, Вам надо найти в пакетах определенные данные. Какая функция Network Monitor позволяет это сделать?

   Задействуйте фильтр Address Pairs (Пары адресов), где укажите MAC-адрес обоих компьютеров. Затем укажите в шестнадцатеричном или ASCII-представлении Pattern Matches (Соответствия шаблону) для фильтрации конкретных шаблонов, содержащихся в кадрах.

6. Ваша цель — гарантировать, что в сети Вашей организации с агентами SNMP могут взаимодействовать лишь две станции управления сетью. Как настроить службу SNMP для усиления зашиты?

   На вкладке Security **(Безопасность) диалогового окна свойств службы SNMP измените** конфигурацию:

   - **залайте уникальное имя сообщества и удалите сообщество Public;**
   - настройте права сообщества так, чтобы NMS могла выполнять включенные функции; если не знаете, какие разрешения сообщества Вам необходимы, разрешите только чтение;
   - **щелкните переключатель** Accept SNMP **packets from those hosts (Принимать** пакеты **SNMP только** от этих **узлов) и укажите имя хоста, IP- или IPX-адрес для каждой NMS;**
   - при посылке ловушек в NMS убедитесь, что на вкладке Traps (Ловушки) указан параметр Trap destination (Адреса назначения ловушки).

Глава 14

Закрепление материала

1. Чем корень DFS отличается от виртуального каталога?

   Термином «виртуальный каталог» обозначают каталоги, вложенные в домашний каталог Web-сервера, но видимые из любого его места. Для описания виртуальных каталогов используются псевдонимы — пользователям обозревателей Web не надо знать о физическом расположении виртуального каталога или пути к нему.

   Корень DFS также обеспечивает централизованный доступ к сетевым ресурсам. Пользователю также не надо знать физическое расположение сетевых ресурсов, он может достигнуть их, перемещаясь от корня DFS, Последний напоминает домашний каталог IIS, а его ресурсы подобны каталогам IIS.

2. Вы открываете документацию по IIS 5.0 из Internet Services Manager (HTML). При этом проблем не возникло. Для доступа к содержащейся в ней информации можно использовать вкладку Index (Указатель). На этой вкладке Вы находите фразу Process Accounting. Однако в результате поиска эта фраза не была найдена. В чем наиболее вероятная причина?

   Служба индексирования была запущена, так как Web-браузер не сообщил о невозможности выполнения поиска. Если фразу не удалось найти, возможно, Вы не настроили службу индексирования для каталогизации папки iisHelp или данная служба не завершила индексирование этой папки.

3. Вы создали виртуальный каталог для WebDAV-публикации. Хотя домашний каталог Web-узла доступен из Internet Explorer 5, доступ к созданному Вами виртуальному каталогу получить не удается. Назовите две причины этой проблемы и возможные пути ее решения.

   Безопасность WebDAV управляет файловой системой и службами IIS, а значит, доступ мог быть запрещен, потому что физический каталог WebDAV имеет ACL, не позволяющий клиенту получить доступ к папке. Если разрешен доступ на уровне файловой системы, про-

верьте, что разрешены чтение, запись н просмотр содержимого виртуального каталога WebDAV. Для поддержки ASP также убедитесь в доступности сценариев.

4. Почему клиент и служба Microsoft Telnet должны поддерживать аутентификацию NTLM?

   Проверка подлинности пользователя, подключенного к серверу Telnet выполняется в контексте текущего системного сеанса. При необходимости аутентификация выполняется по схеме NTLM запрос/ответ. Это важная функция безопасности Telnet в Windows 2000.

5. Какие функции при отсутствии лицензий могут выполнять службы терминалов и как долго?

   Режим Remote Administration (Удаленное администрирование) поддерживает две удаленные управляющие сессии с компьютерами под управлением служб терминалов. Для этого не нужно лицензировать клиент служб терминалов. В режиме Application Server (Сервер приложений) необходимо лицензировать каждую сессию. Службы терминалов будут в течение 90 дней работать без установки клиентских лицензий на сервере лицензий.

ПРИЛОЖЕНИЕ Б

Установка пакетов обновлений

Windows 2000 поддерживает параллельную установку ОС и пакетов исправлений, т. е, пакет в ходе установки добавляется прямо в дистрибутивную папку ОС.

Windows 2000 также устраняет необходимость переустанавливать компоненты, активизированные до установки пакетов исправлений. В прошлом же при обновлении ОС многие ранее установленные компоненты приходилось переустанавливать. Например, в Windows NT 4.0 требовалось переустановить службы IPX и RAS.

Параллельная установка пакетов обновлений

Подразумевает интеграцию пакетов исправлений с версией Windows 2000 на компакт-диске или сетевом ресурсе. При установке Windows 2000 из любого источника соответствующие файлы пакета устанавливаются автоматически.

Для установки нового пакета исправлений служит программа update.exe с ключом /slip — она копирует обновленные файлы из пакета поверх имеющихся файлов Windows 2000. Вот наиболее важные заменяемые файлы:

- layout.inf, dosnet.inf и txtsetup.sif с обновленными контрольными суммами для всех пакетов исправлений; в них включаются записи для всех добавляемых в ходе обновления файлов;
- **архив driver.cab, если в нем изменились** драйверы.

Обновление имеющейся ОС

Пакет обновлений применяется к имеющейся системе Windows 2000 путем запуска update.exe. При изменении состояния ОС (в результате добавления или удаления служб) исходная система уведомляется об установке пакета обновлений: какие файлы заменены/обновлены и откуда устанавливался пакет. Благодаря этому система знает, какие файлы добавлялись из пакета, а какие — из дистрибутива ОС. Если уже после применения пикета состояние системы изменится (например, добавится служба RAS), Windows 2000 установит нужные файлы с дистрибутивного компакт-диска либо из пакета обновлений.

Предметный указатель

S

C

T

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ MICROSOFT

прилагаемый к книге компакт-диск

ЭТО ВАЖНО — ПРОЧИТАЙТЕ ВНИМАТЕЛЬНО. Настоящее лицензионное соглашение (далее «Соглашение») является юридическим документом, оно заключается между Вами (физическим или юридическим лицом) и Microsoft Corporation (далее «корпорация Microsoft») на указанный выше продукт Microsoft, который включает программное обеспечение и может включать сопутствующие мультимедийные и печатные материалы, а также электронную документацию (далее «Программный Продукт»). Любой компонент, входящий в Программный Продукт, который сопровождается отдельным Соглашением, подпадает под действие именно того Соглашения, а не условий, изложенных ниже. Установка, копирование или иное использование данного Программного Продукта означает принятие Вами данного Соглашения, Если Вы не принимаете его условия, то не имеете права устанавливать, копировать или как-то иначе использовать этот Программный Продукт.

ЛИЦЕНЗИЯ НА ПРОГРАММНЫЙ ПРОДУКТ

Программный Продукт защищен законами Соединенных Штатов по авторскому праву и международными договорами по авторскому праву, а также другими законами и договорами по правам на интеллектуальную собственность.

1. **ОБЪЕМ ЛИЦЕНЗИИ.** Настоящее Соглашение дает Вам право:
   a) **Программный продукт.** Вы можете установить и использовать одну копию Программного Продукта на одном компьютере. Основной пользователь компьютера, на котором установлен данный Программный Продукт, может сделать только для себя вторую копию и использовать ее на портативном компьютере.
   b) **Хранение или использование в сети.** Вы можете также скопировать или установить экземпляр Программного Продукта на устройстве хранения, например на сетевом сервере, исключительно для установки или запуска данного Программного Продукта на других компьютерах в своей внутренней сети, но тогда Вы должны приобрести лицензии на каждый такой компьютер. Лицензию на данный Программный продукт нельзя использовать совместно или одновременно на других компьютерах,
   c) **License Pak.** Если Вы купили эту лицензию в составе Microsoft License Pak, можете сделать ряд дополнительных копий программного обеспечения, входяшего в данный Программный Продукт, и использовать каждую копию так, как было описано выше. Кроме того, Вы получаете право сделать соответствующее число вторичных копий для портативного компьютера в целях, также оговоренных выше.
   d) **Примеры кода.** Это относится исключительно к отдельным частям Программною Продукта, заявленным как примеры кола (далее «Примеры»), если таковые входят в состав Программного Продукта.
      i) **Использование и модификация.** Microsoft дает Вам право использовать и модифицировать исходный код Примеров при условии соблюдения пункта (d)(iii) ниже. Вы не имеете права распространять в виде исходного кода ни Примеры, ни их модифицированную версию,
      ii) **Распространяемые файлы.** При соблюдении пункта (d)(iii) Microsoft дает Вам право на свободное от отчислений копирование и распространение в виде объектного кода Примеров или их модифицированной версии, кроме тех частей (или их модифицированных версий), которые оговорены в файле Readme, относящемся к данному Программному Продукту, как не подлежащие распространению.
      iii) **Требования к распространению файлов. Вы** можете распространять файлы, разрешенные к распространению, при условии, что: а) распространяете их в виде объектного кода только в сочетании со своим приложением и как его часть; б) не используете название, эмблему или товарные знаки Microsoft для продвижения своего приложения; в) включаете имеющуюся в Программном Продукте ссылку на авторские права в состав этикетки и заставки своего приложения; г) согласны освободить от ответственности и взять на себя защиту корпорации Microsoft от любых претензий или преследований по закону, включая судебные издержки, если таковые возникнут в результате использов ния или распространения Вашего приложения; и д) не допускаете дальнейшего распространения ко печным пользователем своего приложения. По поводу отчислений и других условий лицензии применительно к иным видам использования или распространения распространяемых файлов обращайтесь в Microsoft.

2. **ПРОЧИЕ ПРАВА И ОГРАНИЧЕНИЯ**
   - **Ограничения на реконструкцию, декомпиляцию и дизассемблирование.** Вы не имеете права реконструировать, декомпилировать или дизассемблировать данный Программный Продукт, кроме того случая, когда такая деятельность (только в той мере, которая необходима) явно разрешается соответствующим законом, несмотря на это ограничение.

- **Разделение компонентов.** Данный Программный Продукт лицензируется как единый продукт. Его компоненты нельзя отделять друг от друга для использования более чем на одном компьютере.
- **Аренда.** Данный Программный Продукт нельзя сдавать в прокат, передавать но временное пользование или уступать для использования в иных целях.
- **Услуги по технической поддержке.** Microsoft может (но не обязана) предоставить Вам услуги по технической поддержке данного **Программного** Продукта (далее «Услуги»). Предоставление Услуг регулируется соответствующими правилами и программами Microsoft, описанными в руководстве пользователя, электронной документации и/или других материалах, публикуемых Microsoft. Любой дополнительный программный код, предоставленный в рамках Услуг, следует считать частью данного Программного Продукта и подпадающим под действие настоящего Соглашения. Что касается технической информации, предоставляемой Вами корпорации Microsoft при использовании ее Услуг, го Microsoft может задействовать эту информацию в деловых целях, в том числе для технической поддержки продукта и разработки. Используя такую техническую информацию, Microsoft не будет ссылаться на Вас.
- **Передача прав на программное обеспечение.** Вы можете безвозвратно уступить все права, регулируемые настоящим Соглашением, при условии, что не оставите себе никаких копий, передадите все составные части данного Программного Продукта (включая компоненты, мультимедийные и печатные материалы, любые обновления, Соглашение и сертификат подлинности, если таковой имеется) и принимающая сторона согласится с условиями настоящего Соглашения.
- **Прекращение действия Соглашения.** Без ущерба для любых других прав Microsoft может прекратить действие настоящего Соглашения, если Вы нарушите его условия. В этом случае Вы должны будете уничтожить все копии данного Программного Продукта вместе со всеми его компонентами.

3. АВТОРСКОЕ ПРАВО. Все авторские права и право собственности на Программный Продукт (в том числе любые изображения, фотографии, анимации, видео, аудио, музыку, текст, примеры кода, распространяемые файлы и апплеты, включенные в состав Программного Продукта) и любые ею копии принадлежат корпорации Microsoft или ее поставщикам. Программный Продукт охраняется законодательством об авторских правах и положениями международных договоров. Таким образом, Вы должны обращаться с данным Программным Продуктом, как с любым другим материалом, охраняемым авторскими правами, с тем исключением, что Вы можете установить Программный Продукт на один компьютер при условии, что храните оригинал исключительно как резервную или архивную копию. Копирование печатных материалов, поставляемых вместе с Программным Продуктом, запрещается

ОГРАНИЧЕНИЕ ГАРАНТИИ

ДАННЫЙ ПРОГРАММНЫЙ ПРОДУКТ (ВКЛЮЧАЯ ИНСТРУКЦИИ ПО ЕГО ИСПОЛЬЗОВАНИЮ) ПРЕДОСТАВЛЯЕТСЯ БЕЗ КАКОЙ-ЛИБО ГАРАНТИИ. КОРПОРАЦИЯ MICROSOFT СНИМАЕТ С СЕБЯ ЛЮБУЮ ВОЗМОЖНУЮ ОТВЕТСТВЕННОСТЬ, В ТОМ ЧИСЛЕ ОТВЕТСТВЕННОСТЬ ЗА КОММЕРЧЕСКУЮ ЦЕННОСТЬ ИЛИ СООТВЕТСТВИЕ ОПРЕДЕЛЕННЫМ ЦЕЛЯМ. ВЕСЬ РИСК ПО ИСПОЛЬЗОВАНИЮ ИЛИ РАБОТЕ С ПРОГРАММНЫМ ПРОДУКТОМ ЛОЖИТСЯ НА ВАС.

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОРПОРАЦИЯ MICROSOFT. ЕЕ РАЗРАБОТЧИКИ, А ТАКЖЕ ВСЕ. ЗАНЯТЫЕ В СОЗДАНИИ, ПРОИЗВОДСТВЕ И РАСПРОСТРАНЕНИИ ДАННОГО ПРОГРАММНОГО ПРОДУКТА, НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКОЙ-ЛИБО УЩЕРБ (ВКЛЮЧАЯ ВСЕ, БЕЗ ИСКЛЮЧЕНИЯ, СЛУЧАИ УПУЩЕННОЙ ВЫГОДЫ, НАРУШЕНИЯ ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ, ПОТЕРИ ИНФОРМАЦИИ ИЛИ ДРУГИХ УБЫТКОВ) ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ИЛИ НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ПРОДУКТА ИЛИ ДОКУМЕНТАЦИИ, ДАЖЕ ЕСЛИ КОРПОРАЦИЯ MICROSOFT БЫЛА ИЗВЕЩЕНА О ВОЗМОЖНОСТИ ТАКИХ ПОТЕРЬ, ТАК КАК В НЕКОТОРЫХ СТРАНАХ НЕ РАЗРЕШЕНО ИСКЛЮЧЕНИЕ ИЛИ ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ ЗА НЕПРЕДНАМЕРЕННЫЙ УЩЕРБ, УКАЗАННОЕ ОГРАНИЧЕНИЕ МОЖЕТ ВАС НЕ КОСНУТЬСЯ.

РАЗНОЕ

Настоящее Соглашение регулируется законодательством штата Вашингтон (США), кроме случаев (и лишь в той мере, насколько это необходимо) исключительной юрисдикции того государства, на территории которого используется Программный Продукт.

Если у Вас возникли какие-либо вопросы, касающиеся настоящего Соглашения, или если Вы желаете связаться с Microsoft по любой другой причине, пожалуйста, обращайтесь в местное представительство Microsoft или пишите по адресу: Microsoft Sales Information Center, One Microsoft Way. Redmond, WA 98052-6399.

Microsoft Corporation

Microsoft Windows 2000 Server

Учебный курс MCSA/MCSE

Издание 4-е, исправленное

Перевод с английского под общей редакцией **А. В. Иванова**

Компьютерный дизайн и подготовка иллюстраций **В. Б. Хильченко**

Технический редактор **О. В. Дергачева**

Дизайнер обложки **Е. В. Козлова**

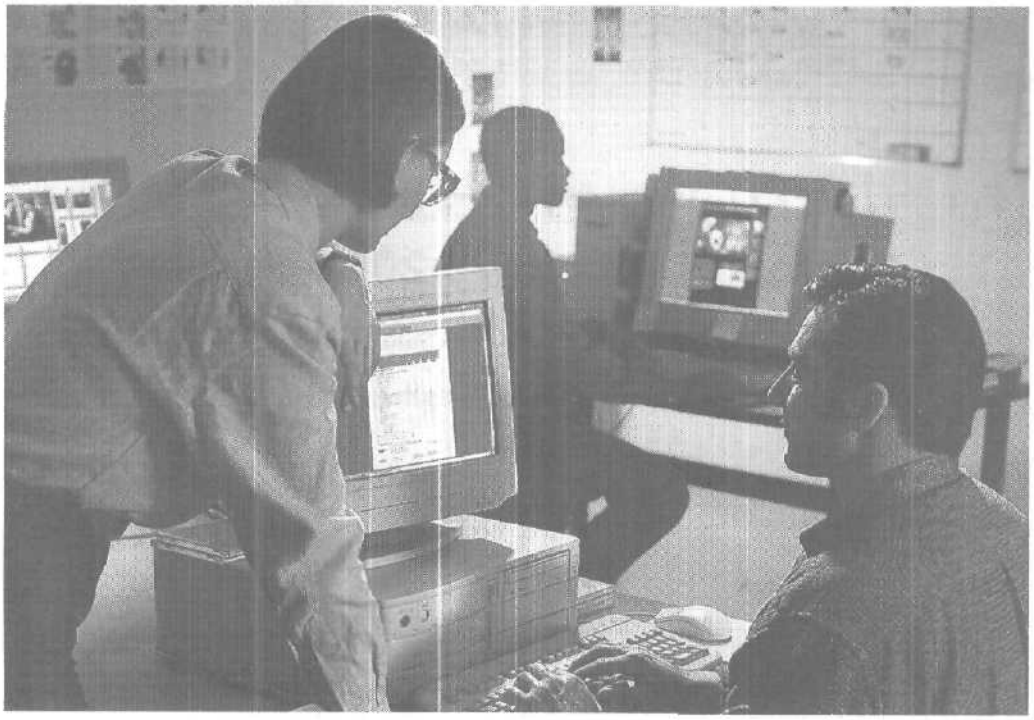
Оригинал-макет выполнен с использованием
издательской системы Adobe PageMaker 6.0

Главный редактор **А. И. Козлов**

Подготовлено к печати издательством «Русская Редакция»
e-mail: info@rusedit.ru, http:// www.rusedit.ru

Подписано в печать 27.08.2003 г. Тираж 2000 экз.
Формат 70x100/16. Физ. п. л. 43

Отпечатано в ОАО «Типография «Новости»,
105005, **г. Москва,** ул. **Фр.** Энгельса, 46



Учебный центр SoftLine

softline education

Ваш курс начинается завтра!

Подготовка сертифицированных инженеров и администраторов Microsoft

Авторизованные и авторские курсы по:

- Windows 2000 / XP
- Sun Solaris 8
- Visual Studio .NET
- Электронной коммерции
- Безопасности информационных систем

и еще более 40 курсов по самым современным компьютерным технологиям.

Дневные и вечерние занятия.

Опытные преподаватели.

Индивидуальные консультации.

Microsoft CERTIFIED Technical Education Center

Учебный центр SoftLine

119991 г. Москва, ул. Губкина, д. 8
тел.: (095) 232 00 23
e-mail: educ@softline.ru
http://education.softline.ru

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
softline
ЛИЦЕНЗИРОВАНИЕ * ОБУЧЕНИЕ * КОНСАЛТИНГ
www.softline.ru • 232 0023 • info@softline.ru

конкурс
«Читатель месяца»

Хотите сэкономить на обучении до $ 1000?

Издательство «Русская Редакция» и учебный центр компании «Инвента» проводят конкурс «Читатель месяца» и будут ежемесячно выбирать двух самых активных читателей книг серии «Учебный курс»,

Просто вырежьте купон из книги, помеченной на обложке специальным значком «Читатель месяца», и пришлите нам по адресу: **123317, Россия, г. Москва, ул. Антонова-Овсеенко, д. 13. Издательство «Русская Редакция».**

Лотерея определит победителей месяца. Один купон — один голос!
Чем больше купонов вы пришлете, тем больше у вас шансов выиграть!

Призы победителям — бесплатное обучение в учебном центре «Инвента» в Москве!

Но это не все! Помимо выбранного вами курса по программе сертификации Microsoft, победителей ждут и другие призы — скидка НЕ дальнейшее обучение в учебном центре и подарок от «Русской Редакции».

Подробности конкурса — на сайте издательстна «Русская Редакция» (*www.rusedit.ru/bonus*) и на сайте компании «Инвента» (*www.inventa.ru*). Там же все новости о конкурсе и о победителях. Телефон для справок (095) 775-8777

Купон участника конкурса «Читатель месяца»

РУССКАЯ РЕДАКЦИЯ ИНВЕНТА

Ф. И. О.:

E-mail:

Телефон:

Род занятий:

ВНИМАНИЕ! Незаполненные купоны не принимаются.

Конкурс *проводится исключительно за счет устроителей* и *данный купон* не может *рассматриваться как коммерческое предложение.*

Купон из книги **Microsoft Windows 2000 Server. Учебный курс MCSA/MCSE**
ISBN 5-7502 0216-X

КОНКУРС