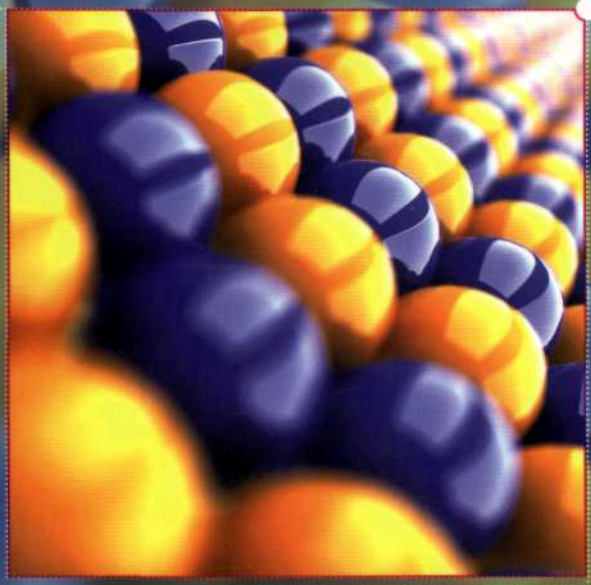
ЕСЛИ ВАМ НУЖНО НАСТРОИТЬ ЛОКАЛЬНУЮ СЕТЬ И СЕРВЕР
НА БАЗЕ WINDOWS SERVER 2003,
ЭТА КНИГА — ВАШ ЛУЧШИЙ ВЫБОР!

ПЕТР ШЕТКА



Microsoft WINDOWS SERVER 2003

Практическое руководство по настройке сети

- # >> От рабочей группы к домену Active Directory
- # >> Готовые решения типичных задач
- # >> Рекомендации профессионалов

ПОЛНОЕ РУКОВОДСТВО

ПЕТР ШЕТКА

Microsoft WINDOWS SERVER 2003

Практическое руководство по настройке сети

Санкт-Петербург, 2006

Шетка Петр

Microsoft Windows Server 2003. Практическое руководство по настройке сети. — СПб.: Наука и Техника, 2006. — 608 с.: ил.

Русское издание под редакцией М.В. Финкова, О.И. Березкиной

ISBN 5-94387-174-8

Серия **«Полное руководство»**

Эта книга представляет собой практическое руководство по развертыванию локальной сети и настройке сервера на основе серверной операционной системы Windows Server 2003. Рассмотрены назначение сетевых служб и их конфигурирование, управление доступом пользователей к сетевым ресурсам, подключение локальной сети к Интернету, удаленный доступ к сети и многое другое. Уделено внимание вопросам выбора, установки и настройки операционных систем для рабочих станций. Отдельно обсуждаются методы и средства повышения эффективности управления сетью, обеспечения ее безопасности.

Книга написана простым и доступным языком, содержит большое количество пошаговых инструкций. Новые понятия, приемы работы и сетевые технологии вводятся поэтапно, по мере возникновения конкретных практических задач, как средства для решения этих задач. На протяжении книги простая одноранговая сеть превращается в домен Active Directory, единообразно управляемый при помощи групповых политик, соединенный с Интернетом и предоставляющий удаленный доступ к своим ресурсам.

Книга отличается своим «практичным» подходом. Предназначена для опытных пользователей и начинающих системных администраторов.

ISBN 5-94387174-8

Контактные телефоны издательства:
(812) 567-70-25, 567-70-26
(044) 516-38-66

Официальный сайт www.nit.com.ru

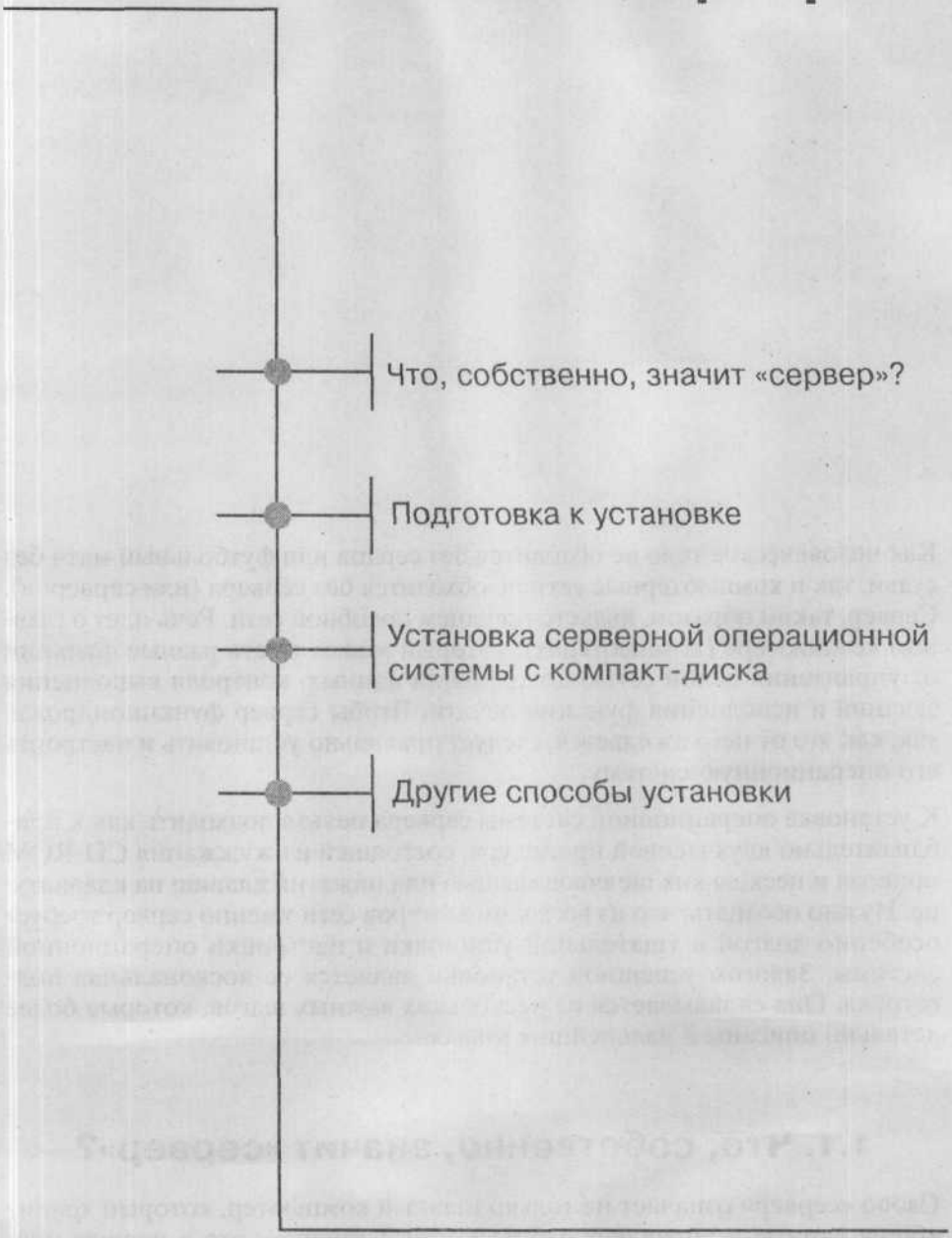
ООО «Наука и Техника»

198097, Санкт-Петербург, ул. Маршала Говорова, 29
Подписано в печать 27.11.2005. Формат 70×100 $^1/_{16}$.
Бумага газетная. Печать офсетная. Объем 38 п. л.
Тираж 5 000 экз. Заказ № 446

Отпечатано с готовых диапозитивов
в ОАО «Техническая книга»
190005, СанктПетербург, Измайловский пр., 29

Содержание

Глава 1 Установка сервера



Как человеческое тело не обходится без сердца или футбольный матч без судьи, так и компьютерные сети не обходятся без сервера (или серверов). Сервер, таким образом, является сердцем подобной сети. Речь идет о главном компьютере (компьютерах), который может иметь разные функции от управления целой сетью до хранения данных, контроля выполнения заданий и исполнения функции печати. Чтобы сервер функционировал так, как это от него ожидается, следует правильно установить и настроить его операционную систему.

К установке операционной системы сервера нельзя подходить как к приблизительно двухчасовой процедуре, состоящей из жужжания CD-ROM привода и нескольких щелчков мышью или нажатий клавиш на клавиатуре. Нужно осознать, что из всех компьютеров сети именно сервер требует особенно долгой и тщательной установки и настройки операционной системы. Залогом успешной установки является ее доскональная подготовка. Она складывается из нескольких важных шагов, которые более детально описаны в дальнейших главах.

1.1. Что, собственно, значит «сервер»?

Слово «сервер» означает не только главный компьютер, который хранит общие данные и управляет работой сети. Сервер — это в первую очередь операционная система, установленная на этом компьютере, а также различные службы и приложения, запущенные на нем и управляющие работой сети.

О каком компьютере можно сказать, что он является сервером? О том, на котором установлена соответствующая операционная система? О том, у которого есть соответствующее аппаратное обеспечение? Или о том, который используется как сервер?

Последний вариант и является правильным. Определение сервера очень просто: речь идет о компьютере, обслуживающем сеть, к которой он подключен (от слова „to serve« — обслуживать). Почти все современные операционные системы могут выполнять некоторые функции сервера. От аппаратной конфигурации зависит мало: сегодня вы часто можете встретить обычные компьютеры, которые оснащены намного лучше, чем сервера (главным образом речь идет о быстродействии процессора и объеме жесткого диска). От чего же тогда зависит, является ли компьютер сервером или нет? Приведем небольшой пример.

Вы только что вернулись из отпуска, в течение которого наснимали множество фотографий своим цифровым фотоаппаратом. Придя на работу, вы сразу скопировали фотографии из фотоаппарата в компьютер. А поскольку вы хотите своими впечатлениями поделиться с коллегами, вы создаете общую папку с разрешением доступа из локальной сети, в которую помещаете свои фотографии. В этот момент ваш компьютер становится сервером для пользователей, обратившихся к этой папке. Кроме того, он выполняет и роль клиента, которую мы рассмотрим в следующей главе. Такой тип сервера называют общим (файловым) сервером.

Однако следует иметь в виду, что, став общим сервером, ваш компьютер получит массу ограничений. С одной стороны, обычные операционные системы (не серверные), могут обеспечить доступ не более чем десяти пользователям одновременно. С другой стороны, может случиться, что, пока ваши коллеги будут рассматривать ваши фотографии, ваш компьютер будет настолько перегружен, что свои обычные функции он будет выполнять слишком медленно или не сможет выполнять вообще.

Чтобы устранить подобные неудобства, для серверов были разработаны специальные операционные системы. Они ориентируются на скорейшее предоставление услуг в сети, при этом использование компьютера в качестве обычной рабочей станции не подразумевается. Правда, пользователь все еще может работать непосредственно за этим компьютером, но графический интерфейс его будет сильно отличаться от привычного интерфейса рабочих станций.

Поскольку в каждой сети возникает необходимость работы с базами данных, файловыми хранилищами, сетевыми принтерами и т. д., то в каждой сети должен присутствовать хотя бы один сервер. Он может совмещать подобные операции. Если все же его оснащение или возложенные на него задачи не позволяют этого сделать, необходимо добавить дополнительные сервера, естественно, с серверными операционными системами.

1.2. Подготовка к установке

Для начала зададим себе несколько вопросов:

- Для каких целей будет использоваться сервер?
- Какую серверную операционную систему следует установить на сервер?
- Какой объем жесткого диска будет требоваться для работы сервера?
- Как должна выглядеть физическая и логическая структура диска?
- Какой тип установки лучше всего подойдет для этого сервера?

Правильные ответы на эти вопросы являются залогом будущей долгой и успешной работы сервера. Некоторые вещи можно подправить уже в процессе работы, другие обязательно установить сразу. Здесь, разумеется, не приводятся все параметры, как, например, объем памяти или скорость и тип процессора. Много ли администраторов в небольших фирмах имеют возможность диктовать свои требования к оборудованию сервера, когда финансированием заведует лицо, не слишком склонное к вложениям в вычислительную технику?

Поскольку далее в этой книге мы рассматриваем небольшую локальную сеть с количеством клиентских мест до 100, то мы назначим сервером обычный компьютер с одним жестким диском. Его быстродействия будет достаточно для поставленных задач.

Подготовка к установке состоит из досконального планирования функций и конфигурации сервера и сбора всех данных, необходимых для установки. Решительно невозможно начать установку без подготовки, собирая необходимые сведения по ходу дела и выдумывая конфигурацию на скорую руку.

Функции сервера

Сервер — это компьютер, который предлагает свои службы в сети. Какие конкретно службы требуются, зависит от конкретной сети и от требований пользовательского коллектива. Сервер может выполнять, к примеру, следующие функции:

- Общего сервера (файлового сервера).
- Сервера базы данных.
- Сервера приложений.
- Терминального сервера.
- Сервера печати.
- Контроллера домена.
- Сервера DNS.
- Сервера WINS.
- Сервера DHCP.

- Почтового сервера.
- Веб-сервера.
- Сервера FTP.
- Сервера NNTP.
- Сервера с опцией удаленной установки (RIS).
- Сервера удаленных соединений.
- Сервера управления сертификатами с сертификационными функциями
- и другие.

Какие-то функции должны выполняться во всех сетях, а какие-то требуются только в некоторых из них. Очень важно решить, какие из функций будут нужны в данной сети, поскольку от этого зависят и остальные требования к установке. Далее, необходимо знать, какие из функций можно без тотального переконфигурирования сервера добавить и потом, а для каких функций следует выделить отдельный компьютер.

В нашей сети мы будем последовательно работать со следующими функциями:

- Общий сервер (файловый сервер).
- Сервер печати.
- Контроллер доменов.
- Сервер DNS.
- Сервер DHCP.
- Сервер удаленных соединений.

С этими функциями может справиться и один компьютер, более того — их можно в любое время удалить и восстановить. В этом отношении установка не будет иметь осложнений, и более подробная информация в данный момент не нужна.

Примечание.

Если вы еще не до конца понимаете все эти термины, ничего страшного. При планировании установки их все равно нельзя будет обойти, и более подробно некоторые из них мы рассмотрим далее.

Какую операционную систему семейства Windows Server 2003 установить?

Члены семейства операционных систем Windows Server 2003 перечислены в. таблице 1.1.

Обзор версий Windows Server 2003 *Таблица 1.1*

Версия системы	Описание
Windows Server 2003, Web Edition	Эта версия предназначена для предоставления локальных служб в сети. Поскольку ее разрабатывали главным образом для веб-приложений, в нее не вошли некоторые важные службы, и поэтому она не предназначена для обычной офисной сети
Windows Server 2003, Standard Edition	Эта версия предназначена для сети организации любой величины. Она обеспечивает все стандартные службы и поэтому действительно является стандартной
Windows Server 2003, Enterprize Edition	Эта версия предназначена для крупной сети. Она поддерживает технологию кластеризации и позволяет работать с ресурсоемкими приложениями и системами распределенного вычисления
Windows Server 2003, Datacenter Edition	Эта версия предназначена для сети с высокими требованиями к безопасности, скорости и масштабируемости. Делает возможным объединение нескольких серверов на одном аппратном обеспечении

У каждой версии есть минимальные системные требования к оборудованию и ограничения по использованию ресурсов (см. таблицу 1.2).

Системные требования и возможности Windows Server 2003 *Таблица 1.2*

Версии системы	Минимальные системные требования
Windows Server 2003, Web Edition	CPU от 133 МГц (рекомендуется 550 МГц), 128 Мб RAM (рекомендуется 256 Мб), 1.5 Гб места на диске. Система поддерживает не более 2 Гб памяти RAM и максимум 2 процессора
Windows Server 2003, Standard Edition	CPU от 133 МГц (рекомендуется 550 МГц), 128 Мб RAM (рекомендуется 256 Мб), 1.5 Гб места на диске. Система поддерживает не более 4 Гб памяти RAM и максимум 4 процессора
Windows Server 2003, Enterprize Edition	CPU от 133 МГц (рекомендуется 733 МГц), 128 Мб RAM (рекомендуется 256 Мб), 1.5 Гб места на диске. Система поддерживает не более 32 Гб памяти RAM и максимум 8 процессоров
Windows Server 2003, Datacenter Edition	CPU от 400 МГц (рекомендуется 733 МГц), 512 Мб RAM (рекомендуется 1 Гб), 1.5 Гб места на диске. Система поддерживает не более 64 Гб памяти RAM и максимум 32 процессора

Для малой или средней сети предназначена версия Windows Server 2003, Standard Edition: с одной стороны, она отвечает требованиям необходимых служб, а с другой, нам ни к чему версия Windows Server 2003 Enterprize Edition, поскольку мы не сможем использовать ее возможности в полном объеме.

Примечание.

Подробную информацию об использовании отдельных служб в версиях системы Windows Server 2003 вы найдете на веб-странице компании Microsoft по адресу http://www.microsoft.com/windowsserver2003/evaluation/choosing/.

Объем диска

Ответ на вопрос, сколько дискового пространства понадобится для выполнения функций сервера, зависит и от того, какие именно функции он будет выполнять, и от размера сети. Требование к объему свободного места на диске, необходимому для самой системы, уже дано разработчиком — 1.5 Гб. Понадобится также место для рабочих файлов системы и для установки будущих обновлений Service Pack: это еще примерно 1 Гб.

Естественно, какое-то место займут установленные приложения. Даже если мы пока не планируем установку сервера базы данных, сервера приложений или почтового сервера, следует помнить об антивирусных программах, настройках безопасности и т.д. Для этих целей и на случай дальнейшего расширения сервера нужно предусмотреть 5 Гб места.

Больше всего места нужно будет оставить непосредственно для файлов, с которыми будут работать пользователи (под файловый сервер). Как известно, места всегда не хватает, и ограничить аппетиты пользователей нужно с помощью системных средств, введя квоты. Это решение должно быть принято в самом начале и сразу же проведено в жизнь. Для обычной работы на компьютере каждому пользователю можно выделить 1 Гб дискового пространства.

Дальнейшие расчеты — дело простой арифметики. Если, например, мы работаем с сетью в 30 пользователей, то нам потребуется около 40 Гб места на диске, что сегодня не представляет проблемы ни с технической, ни с финансовой стороны.

Если вы собрались купить новый компьютер для использования его в качестве сервера и ваше мнение учитывается при выборе его конфигурации, я рекомендую остановиться на такой, в которую потом можно было бы добавить жесткий диск, и не один. Таким образом вы обеспечите себе возможность в дальнейшем использовать этот компьютер и как сервер базы данных или сервер приложений.

Дисковая конфигурация

Мы подходим к одному из важнейших шагов. При выборе конфигурации дисков системный администратор чаще всего сталкивается с финансовыми и техническими ограничениями: дисков либо мало, либо новые диски некуда подключить. Если же от этих ограничений отвлечься, то руководствоваться нужно несколькими простыми и понятными правилами:

- Операционная система не должна размещаться на том же диске, что и настройки безопасности.
- Данные приложений (файлы, созданные пользователями) должны быть отделены от системы и приложений. В случае приложений базы

данных нужно иметь дополнительный жесткий диск для протоколов транзакций.

- Для повышения надежности операционной системы и защиты данных рекомендуется применить дисковые структуры, устойчивые к ошибкам (зеркальные массивы, массивы типа RAID-5).

О разбиении дисков на логические разделы единого мнения среди системных администраторов нет. Одни считают, что в целях безопасности и простоты переустановки необходимо держать операционную систему, приложения и пользовательские данные на разных логических дисках. Другие подчеркивают, что на неразделенном диске можно хранить огромные файлы: архивы, базы данных, видеоизображение.

Примечание редактора.

Все же на практике лучше разделять диски на логические и отводить под пользовательские данные отдельный раздел. Таким образом можно сэкономить на резервном копировании, архивируя только пользовательский раздел, а операционную систему и приложения в случае какого-либо сбоя переустанавливая заново.

В нашем случае мы исходим из самого простого решения: берем один физический диск и разбиваем на три логических раздела — C:, D: и E:. Устанавливать систему будем на диск C:.

С точки зрения производительности это решение не оптимально, зато оно дешево и вполне достаточно для небольшой сети. О других возможных конфигурациях будет рассказано в главах, посвященных функциям, связанным с дисками.

Тип установки

Существуют разные типы установки операционных систем Microsoft: от классической, хорошо известной установки с компакт-диска до автоматической установки или установки посредством клонирования дисков.

Автоматически установить Windows Server 2003 можно на компьютер, на котором сейчас стоит Windows XP Professional (для Windows 2000 Server необходима Windows Professional 2000).

Однако если перед вами стоит задача установки серверной операционной системы на чистый компьютер, вам не останется ничего другого, кроме обычной установки с CD-ROM. То есть в первый раз вам придется честно пройти весь процесс установки, чтобы подготовить возможность автоустановки на будущее.

Сбор информации, необходимой для установки

Во время самой установки вы должны будете ввести сведения, которые полезно приготовить заранее. Некоторые из этих данных значения не имеют, а другие, наоборот, очень важны, потому что от них критически зависит работа системы, а исправить их позже будет невозможно.

Итак, подготовьте следующую информацию:

- Имя пользователя и название организации, на которую зарегистрирован продукт.
- Тип лицензирования клиентского доступа.
- Код **Product Key** (как правило, он находится на обратной стороне обложки CD-ROM).
- Имя компьютера.
- Пароль администратора.
- Имя рабочей группы, в которую будет включен компьютер.

На некоторых понятиях мы еще остановимся в процессе установки и разъясним их подробнее.

1.3. Установка серверной операционной системы с компакт-диска

Эта глава содержит подробное описание установки, включая важные диалоговые окна и дополнительные картинки. Для успешной установки вам потребуется установочный диск CD-ROM с операционной системой Windows Server 2003, Standard Edition и «чистый» компьютер.

Примечание редактора.

Каждому понятно, что работать с локализованной версией операционной системы проще и удобнее. Но локализованная версия — это исправленная версия, не застрахованная от появления новых ошибок. Поэтому правильнее и надежнее будет сначала установить нелокализованную (английскую) версию, а сверху уже ставить пакет MUI (Multilingual User Interface) для русификации. Потом для того, чтобы все надписи отображались на русском языке, надо в **Панели управления** открыть диалоговое окно **Язык и региональные настройки** и выбрать русский язык. Далее в этой главе будет приведено пошаговое описание необходимых действий. А пока при описании установки английские названия команд и окон будут дублироваться русскими.

1. В настройках BIOS установите следующую последовательность загрузки с устройств:
   - CD-ROM.
   - Жесткий диск.

Эта настройка всегда зависит от типа BIOS, поэтому ее нельзя описать универсально. Подробную информацию вы найдете в описании, прилагающемся к вашей материнской плате.

2. В привод CD-ROM вставьте установочный компакт-диск с операционной системой Windows Server 2003 и перезагрузите компьютер.
3. Установка системы должна начаться автоматически. Если этого не происходит, проверьте еще раз порядок загрузки в BIOS. Если же в компьютере уже была установлена какая-то операционная система, может случиться так, что для начала установки системе будет требоваться нажатие любой клавиши.
4. Включится текстовый режим установки и появится окно с надписью **Windows Server 2003 Setup (Установка операционной системы Windows)**.
5. В окне **Welcome To Setup (Вас приветствует программа установки)** нажмите клавишу **Enter**.
6. В окне **Windows Licensing Agreement (Лицензионное соглашение Windows)** подтвердите нажатием клавиши **F8** согласие с условиями лицензии.

Примечание.

Перед нажатием клавиши F8 вы можете углубиться в изучение договора о лицензировании и, найдя в нем нечто вас не устраивающее, прервать установку нажатием клавиши Esc.

7. В следующем окне нужно создать (или изменить) логическую структуру жесткого диска. Нажмите клавишу **C**, что позволит вам создать раздел для установки операционной системы или, если раздел уже существует, выберите его из списка и нажмите **Enter**.
8. В части **Create a Partition (Создать раздел объёма)** отображен максимально доступный объем жесткого диска. Если в вашем сервере только один диск, укажите 10240 Мб (то есть 10 Гб). Таким образом, останется место, необходимое для файлов пользователей. Если в вашем компьютере несколько жёстких дисков, можете оставить максимальный предложенный объём. Потом нажмите клавишу **Enter**.
9. В списке разделов вновь созданный раздел должен быть обозначен как раздел **C:**. Если это не так, назначьте ему букву C: и нажмите клавишу **Enter**.
10. В следующем диалоговом окне вы можете выбрать файловую систему, которую следует создать на новом разделе. Если вы не сомневаетесь в качестве поверхности диска, установите переключатель в положение **Format in NTFS File System (Quick) (Отформатировать раздел файловой системой NTFS (Быстро))** — так вы сэкономите время. Если у вас есть сомнения, выберите положение **Format in**

NTFS File System (Отформатировать раздел файловой системой NTFS). В этом случае при форматировании будет произведен физический контроль поверхности и поврежденные («bad») блоки будут исключены из использования. После форматирования раздела начнется копирование файлов в папку установки системы Windows Server 2003.

11. После копирования файлов будет произведена перезагрузка, и установка будет продолжена в графическом режиме.
12. В диалоговом окне **Regional and Language Options (Язык и региональные стандарты)** (см. рис. 1.1) выберите подходящие региональные настройки (язык, формат дат и времени, денежные единицы) и раскладку клавиатуры и нажмите кнопку **Next (Далее)**.
13. В диалоговом окне **Personalize Your Software (Ввод данных пользователя)** (см. рис. 1.2) введите данные, которые вы подготовили перед началом установки, а затем нажмите кнопку **Next (Далее)**.

Примечание.

Имя пользователя и название организации можно будет в любое время изменить вмешательством в системный реестр. Эти параметры находятся в ветви HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion. Но будьте аккуратны, повреждение реестра может повлечь за собой выход из строя всей операционной системы.

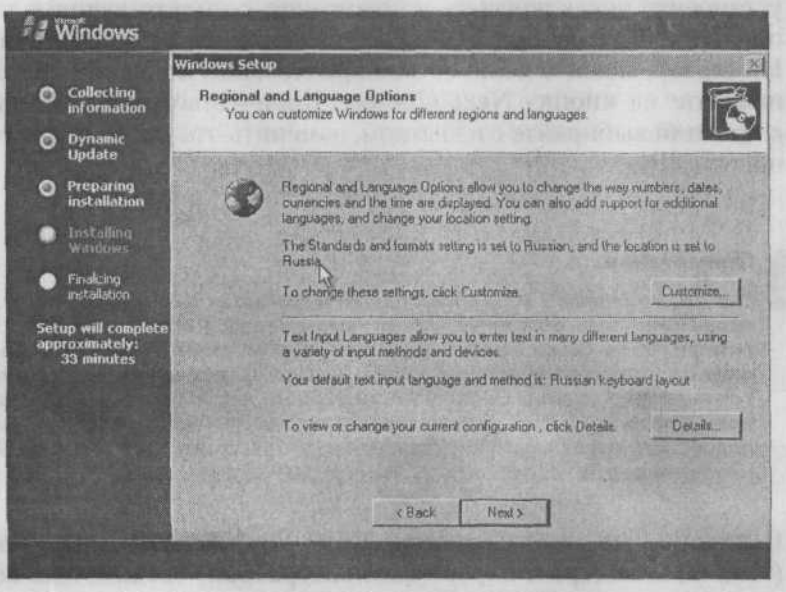


Рис. 1.1.** Диалоговое окно **Язык и региональные стандарты

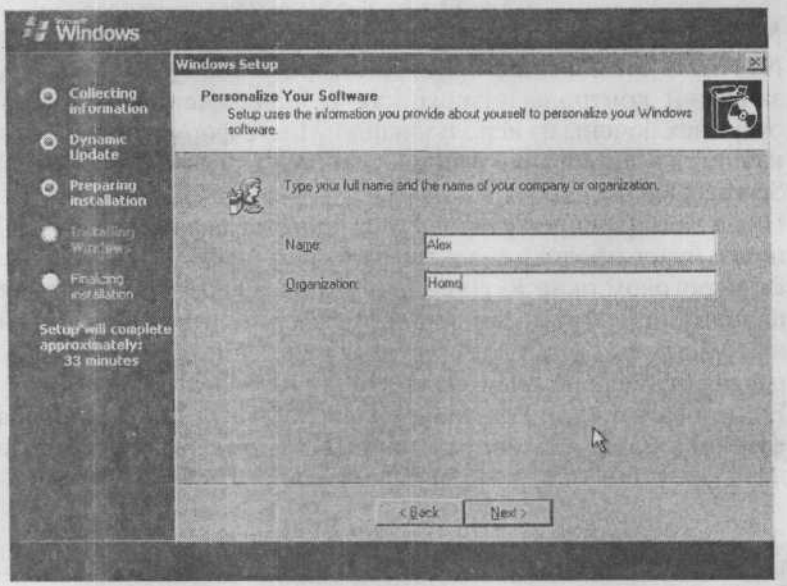


Рис. 1.2. Диалоговое окно ***Ввод данных пользователя***

14. В диалоговом окне **Product Key (Код продукта)** (см. рис. 1.3) введите код для установки операционной системы и нажмите кнопку **Next (Далее)**.
15. В диалоговом окне **Licensing Modes (Способ регистрации лицензии)** установите переключатель в положение, соответствующее типу лицензирования, который вы выбрали. Если вы оставляете значение **На сервер**, задайте количество параллельных подключений, а затем нажмите на кнопку **Next (Далее)**. Количество параллельных подключений выбирайте с избытком, изменить это число в дальнейшем невозможно.

Примечание.

Тип лицензирования **На сервер** делает возможным параллельное подключение заданного числа пользовательских компьютеров. Любая попытка добавления компьютеров сверх лимита будет сервером отвергаться. При настройке лицензирования **На устройство** максимальное число параллельных подключений компьютеров задано купленной лицензией, как и при лицензировании **На пользователя**, но с учетом количества пользователей, а не компьютеров. Более подробную информацию о лицензировании продукта Microsoft вы найдете на `http://www.microsoft.com/windowsserver2003/howtobuy/licensing`.

16. В диалоговом окне **Computer Name And Administrator Password (Имя компьютера и пароль администратора)** введите имя компьютера (например, **SRVR001**) и пароль администратора (например,

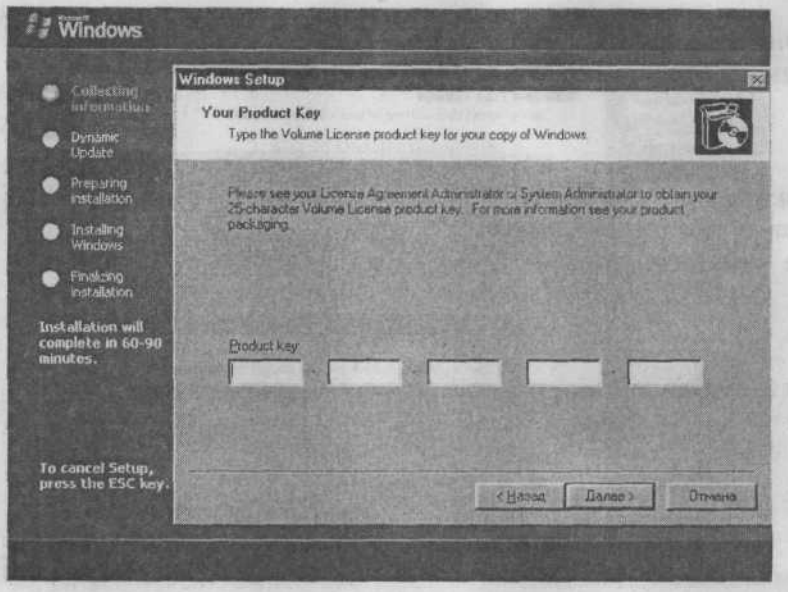


Рис. 1.3. *Ввод кода Product Key*

K@l!na — будьте внимательны, пароль различает прописные и строчные буквы). Продолжите нажатием кнопки **Next (Далее)**.

Примечание.

Безопасными (отвечающими требованиям сложности) считаются пароли, в которых перемешаны заглавные и строчные буквы, цифры и знаки препинания. Обратите внимание на то, как получился пароль в нашем примере: мы взяли слово, которое легко запомнить («калина») и заменили в нем некоторые символы, так что его стало трудно подобрать. Вы можете воспользоваться этой методикой составления паролей или придумать свою.

17. В диалоговом окне **Date And Time Settings (Установка даты и времени)** (см. рис.1.4) введите текущую дату, время и выберите нужный часовой пояс. Продолжите нажатием на кнопку **Next (Далее)**.
18. В диалоговом окне **Network Settings (Установки сети)** (см. рис 1.5) отметьте поле **Custom settings (Особые настройки)** и затем нажмите на кнопку **Next (Далее)**.
19. В диалоговом окне **Networking Components (Настройки сети)** выберите строку **Internet Protocol (TCP/IP) (Протокол сети Интернет (TCP/IP))**, а затем нажмите на кнопку **Properties (Свойства)**.
20. В диалоговом окне **Internet Protocol (TCP/IP) (Протокол сети Интернет (TCP/IP)) — Properties (Свойства)** (см. рис. 1.6) введите адрес IP 192.168.10.2 и маску подсети 255.255.255.0. Остальные свой-

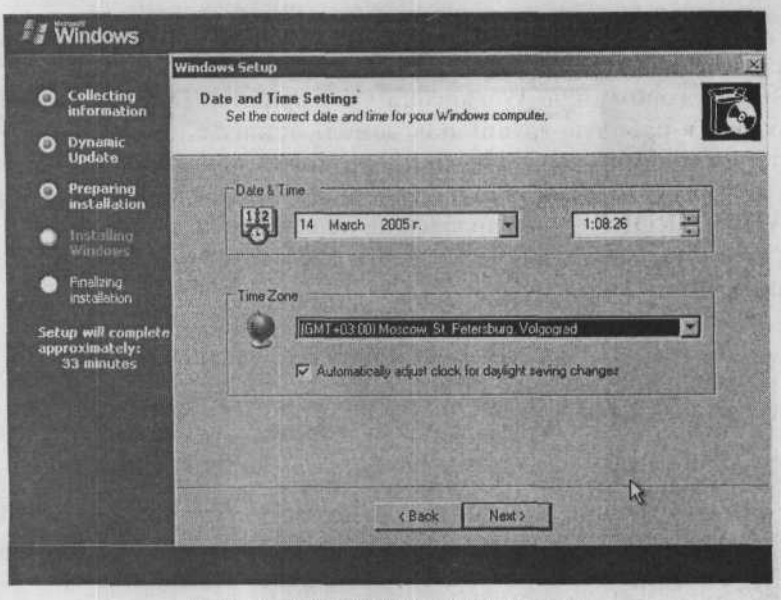


Рис. 1.4. *Установка даты и времени*

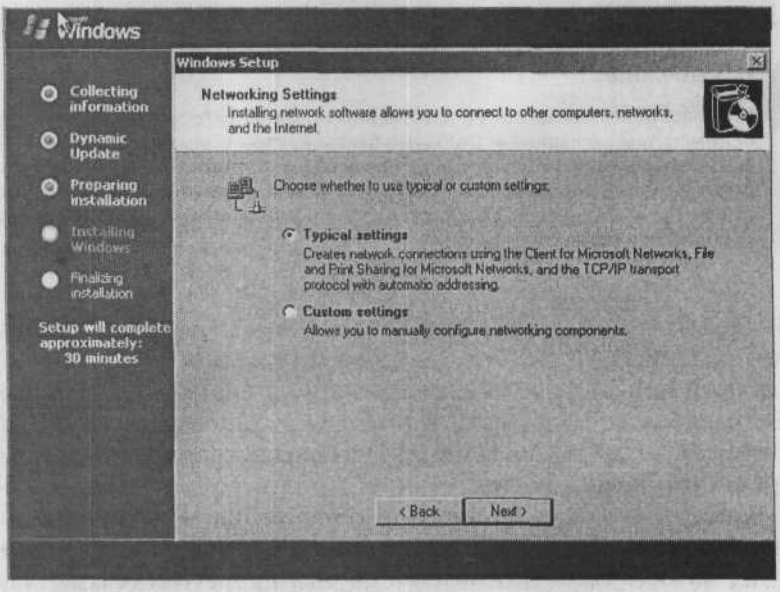


Рис. 1.5. *Установка сети*

ства не отмечайте и нажмите на кнопку **OK**. Продолжите нажатием на кнопку **Next (Далее)**.

21. В диалоговом окне **Workgroup Or Computer Domain (Компьютер входит в рабочую группу или домен)** оставьте исходные настройки (т.е. отмеченное поле **No, this computer is not on a network, or is on a network without a domain. Make this computer a member of a group: WORKGROUP — Компьютер не подключён к сети или подключён к сети без домена и будет членом следующей группы ГРУППА**) и нажмите на кнопку **Next (Далее)**.

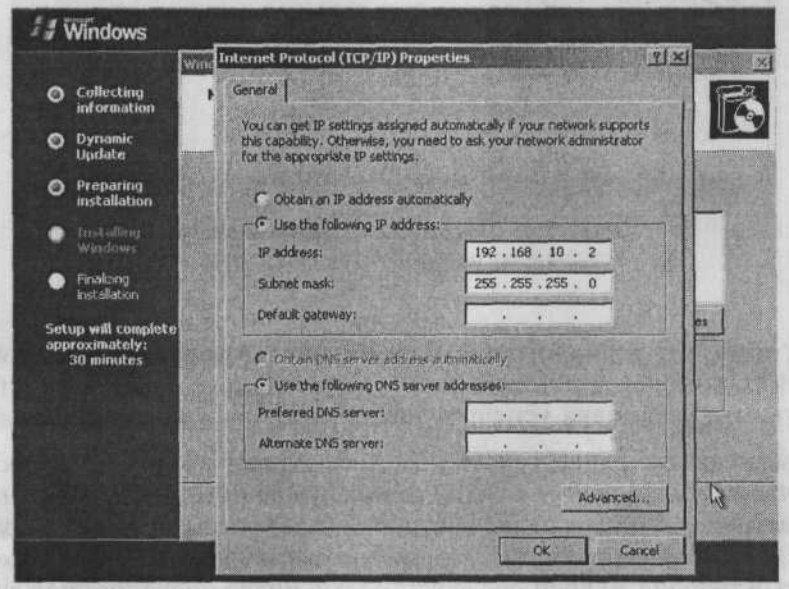


Рис. 1.6. *Конфигурация адреса и других параметров протокола IP*

После задания этих параметров начнется установка системы. По завершении установки компьютер будет перезагружен.

Действия после установки

Поскольку Windows Server 2003 — сравнительно новая операционная система, она может не содержать драйверов для некоторых установленных у вас устройств. Список оборудования, совместимого с Windows Server 2003 (Hardware Compatibility List), можно найти на `http://www.microsoft.com/hcl`. Если ваши устройства в этом списке отсутствуют, замените их или попытайтесь получить необходимые драйверы у производителей и установите их вручную. Когда вы при-

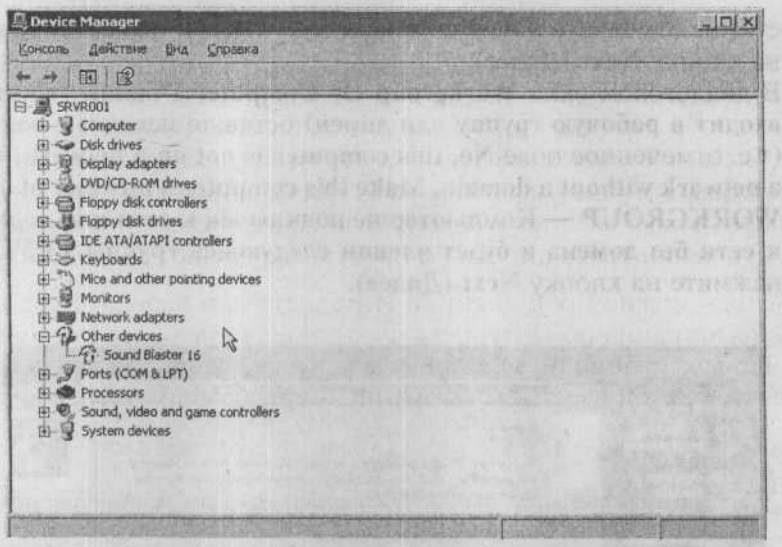


Рис. 1.7. *Список оборудования — видно, что драйвер звуковой карты не установлен*

дете к тому, что в диалоговом окне **Диспетчер устройств** не появится ни одного вопросительного или восклицательного знака, можно будет сказать, что установка успешно завершена.

Как было сказано ранее, сервер может выполнять различные функции, и ясно, что для выполнения каждой из них нужно произвести дополнительную настройку. Продолжение настройки будет рассмотрено в следующих главах. После настройки продукт нужно активировать. Это необходимо сделать в течение 30 дней после установки, иначе операционная система перестанет работать. Только с момента активации Windows Server 2003 начнет функционировать без ограничений.

Остановимся на активации подробнее.

Активация системы

Система Windows Server 2003 содержит функцию, названную **Активация системы Windows (WPA, Windows Product Activation)**. Она является еще одним из средств, применяемых компанией Microsoft в борьбе с нарушителями авторских прав, и препятствует установке одного и того же дистрибутива системы на разные компьютеры.

При установке системы вы должны были ввести код Product Key из 25 символов. Система Windows Server 2003 сгенерирует еще один код на основе характеристик оборудования вашего компьютера. Активация системы со-

стоит в том, что вы посылаете код, полученный соединением Product Key и кода оборудования, в центр Microsoft Clearinghouse. Там выясняют, действительно ли компания Microsoft выпустила продукт с таким Product Key и верно ли, что эта система не была установлена (точнее, активирована) ранее. Если ответ положительный, то Microsoft Clearinghouse пришлет вам подтверждающий идентификатор из 42 символов, который для завершения активации нужно ввести в систему. Если подтверждающий код не введен, то по истечении срока активации продукт перестанет функционировать.

Активацию можно произвести по Интернету или передать код по телефону. Регистрация по Интернету продолжается не более нескольких секунд. При активации по телефону вы должны будете сообщить код из 50 символов, а затем ввести в систему подтверждающий идентификатор.

Совет.

Не слишком спешите с активацией продукта: сначала сконфигурируйте систему и все оборудование и погоняйте сервер хотя бы неделю, чтобы убедиться, что он работает правильно и никаких устройств заменять не нужно. Месячный срок активации предоставляется именно для этой цели. Если после активации вы замените какие-то устройства, то вам придется производить активацию заново, с новым кодом оборудования.

1.4. Другие способы установки

Windows Server 2003, как и ее предшественница Windows Server 2000, поддерживает несколько возможностей, и в этом параграфе мы их перечислим.

Установка по сети

Установка по сети не слишком отличается от установки с компакт-диска. Необходимо выполнить следующие подготовительные действия:

- Создать сетевую папку, содержащую установочные компоненты операционной системы.
- На компьютере, на который вы хотите установить систему, запустить сетевого клиента.
- На жестком диске компьютера, на который будет производиться установка, создать раздел объемом по крайней мере 1.5 Гб.

Установка без обслуживания (по сети или с компакт-диска)

Этот тип установки подробно рассмотрен в следующей главе. Вкратце, нужно подготовить текстовый файл специального формата с ответами на

вопросы, задаваемые инсталлятором системы, и передать его программе установки как параметр.

Преимуществом такого типа установки является существенная экономия времени: не нужно сидеть у компьютера и ждать, когда появится следующее диалоговое окно. Чаще всего таким способом операционная система устанавливается на клиентские компьютеры, но возможен он и для серверов.

Клонирование дисков

У всех предыдущих способов установки есть один недостаток: настраивать операционную систему и приложения приходится на каждом компьютере отдельно. Клонирование, или дублирование, дисков это неудобство устраняет. Вы можете установить систему и приложения на компьютер-оригинал, настроить их и скопировать жесткий диск бит в бит на диск другого компьютера. Этот способ выгодно использовать для настройки большого количества рабочих станций.

Перед дублированием диска нужно запустить на компьютере-оригинале утилиту SYSPREP (**Подготовка системы**), которая выберет уникальные идентификаторы системы (например, имя компьютера) и обеспечит их создание при дальнейшем запуске.

Для серверных операционных систем этот способ установки не используется. Более того, компания Microsoft не предоставляет никаких утилит для воссоздания битовой копии диска на другом компьютере. Для этого приходится применить утилиты от других разработчиков.

Удаленная установка

Это особый случай установки, рассмотренный в главе 19. Windows Server 2003 является первой серверной системой, которую можно установить таким способом. Служба удаленной установки в Windows 2000 Server делала возможной только установку операционной системы для клиентских компьютеров Windows 2000 Professional.

Русификация операционной системы

Для того чтобы работать в привычной нам среде с русскоязычными командами меню и диалоговыми окнами, необходимо установить пакет MUI (Multilingual User Interface) поддержки многоязыкового интерфейса. Запустите программу установки, обычно расположенную в папке MUI и называющуюся `muisetup.exe`. После запуска появится окно с лицензионным соглашением (рис. 1.8).

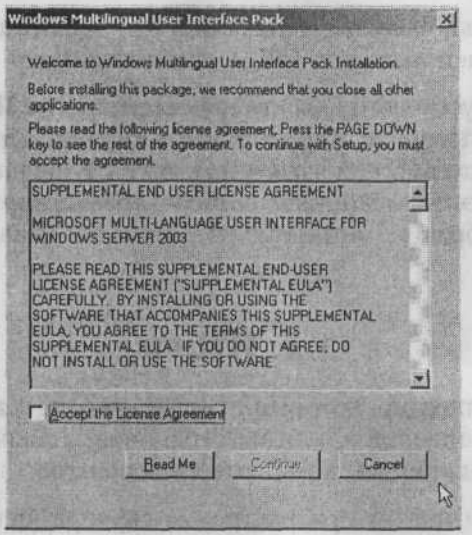


Рис. 1.8. *Начало установки MUI. Лицензионное соглашение*

Нужно отметить галочкой свое согласие с условиями и нажать **Continue (Продолжить)**. После этого отобразится окно выбора языков (рис. 1.9).

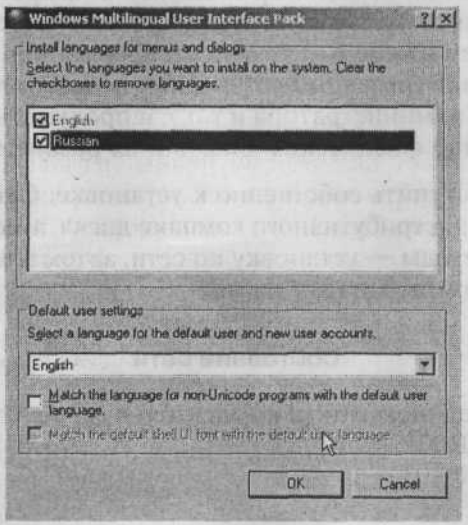


Рис. 1.9. *Выбор языков*

Выберите из списка язык по умолчанию для всех будущих учетных записей пользователей, нажмите OK, и установка будет произведена.

Чтобы включить русскоязычный интерфейс, откройте **Панель управления** (**Control Panel**), выберите **Regional and Language Options**, на вкладке **Languages** выберите русский язык и нажмите **OK** для применения новых установок. После этого закончите сеанс и зарегистрируйтесь снова. При входе в систему обратите внимание на раскладку клавиатуры.

1.5. Итоги

Сервер — это компьютер, который предлагает в сети свои услуги клиентам. Количество серверов в сети не ограничено, обычно, правда, их на пару порядков меньше, чем компьютеров-клиентов.

Особенно важным шагом при настройке сервера является выбор правильной операционной системы. В большинстве случаев, учитывая возможность дальнейшего увеличения количества компьютеров-клиентов, достаточной будет операционная система Windows Server 2003, Standard Edition. Большие сети с непростыми приложениями могут обеспечиваться сервером с Windows Server 2003, Enterprise Edition. Для тех, кто предоставляет Интернет-услуги или устраивает Интернет-презентации, предназначена Windows Server 2003, Web Edition.

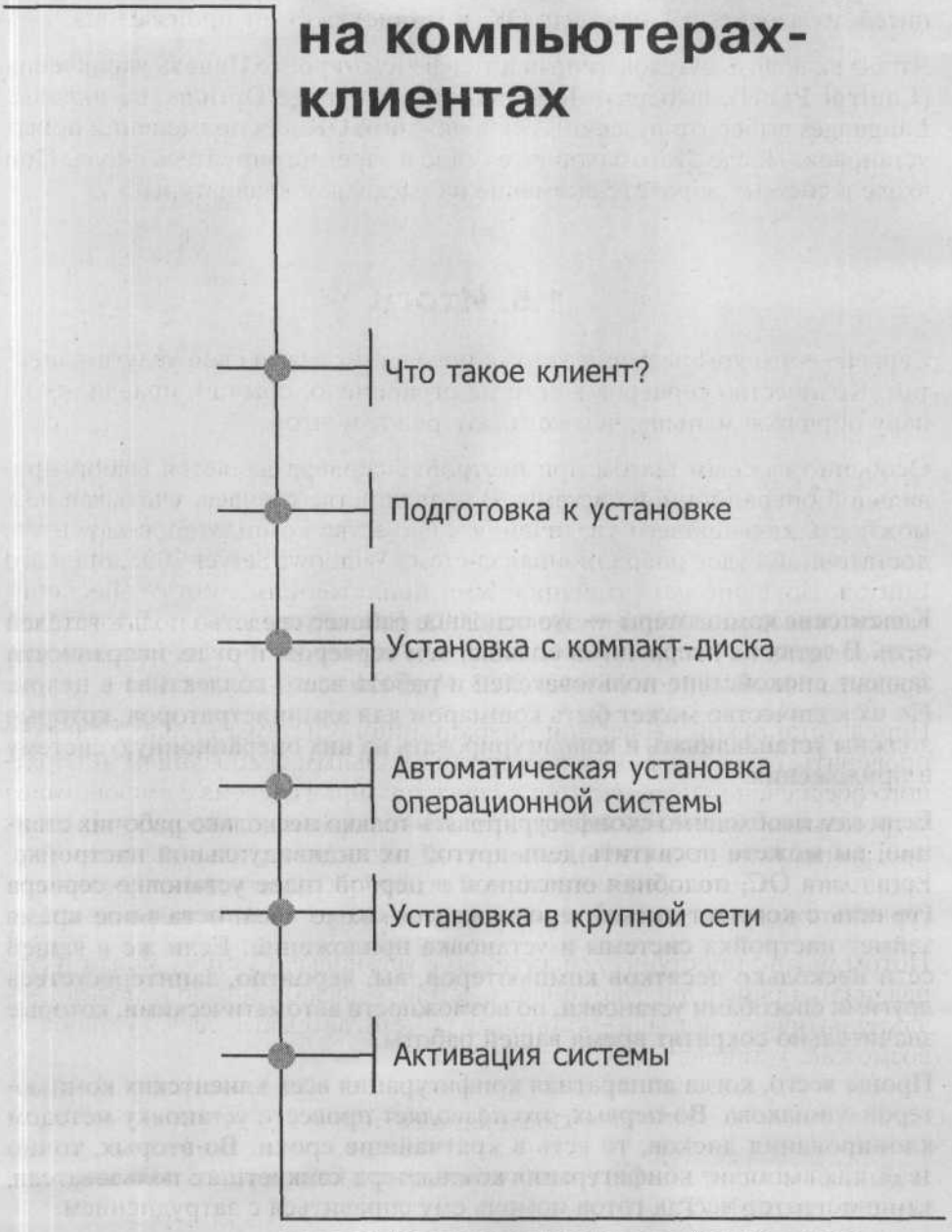
Перед установкой серверной операционной системы вначале следует проверить, отвечает ли компьютер минимальным требованиям аппаратного обеспечения и совместима ли операционная система с имеющимися устройствами. Затем нужно подготовить информацию, которую запросит программа установки (имя компьютера, имя пользователя и название организации, пароль администратора и т.п.), и продумать дисковую конфигурацию (количество физических дисков и их разбиение на разделы).

Потом можно приступить собственно к установке. Систему можно устанавливать прямо с дистрибутивного компакт-диска, а можно использовать альтернативные методы — установку по сети, автоматическую установку, возможно, установку дубликата дисков.

Состояние сети

В данный момент единственный компьютер в сети с установками — сервер с именем SRVR001.

Глава 2 Установка ОС на компьютерах-клиентах



Клиентские компьютеры — это основное рабочее средство пользователей сети. В сетях их несравнимо больше, чем серверов, и от их исправности зависит спокойствие пользователей и работа всего коллектива в целом. Но их количество может быть кошмаром для администраторов, которые должны устанавливать и конфигурировать на них операционную систему и приложения.

Если вам необходимо сконфигурировать только несколько рабочих станций, вы можете посвятить день-другой их индивидуальной настройке. Установка ОС, подобная описанной в первой главе установке сервера (то есть с компакт-диска), продолжается около часа, остальное время займет настройка системы и установка приложений. Если же в вашей сети несколько десятков компьютеров, вы, вероятно, заинтересуетесь другими способами установки, по возможности автоматическими, которые значительно сократят время вашей работы.

Проще всего, когда аппаратная конфигурация всех клиентских компьютеров одинакова. Во-первых, это позволяет провести установку методом клонирования дисков, то есть в кратчайшие сроки. Во-вторых, точно зная, как выглядит конфигурация компьютера конкретного пользователя, администратор всегда готов помочь ему справиться с затруднением.

В этой главе мы рассмотрим разные способы установки ОС на клиентские компьютеры и подробно обсудим, как эту установку проводить.

2.1. Что такое клиент?

Клиент — это компьютер, который является противоположностью сервера. Если сервер предлагает в сети свои услуги, то клиент этими услугами пользуется. Примером такого использования может служить доступ к документам, расположенным на сервере, печать на принтерах, подключенных к серверам печати или, например, запрос IP-адреса у DHCP-сервера.

Клиентская роль компьютера не зависит от того, какая ОС на нем установлена. В сети организации на рабочие станции следует устанавливать Windows XP Professional или по крайней мере Windows 2000 Professional.

Компьютер-клиент может оказаться и в роли сервера: например, когда вы разрешаете своим коллегам доступ к вашему диску с целью проведения собрания или позволяете им печатать на принтере, подключенном к вашему компьютеру. Однако такие случаи являются скорее исключением и, если вы все же собираетесь ими воспользоваться, помните, что клиентская операционная система разрешает одновременное подключение не более чем 10 «вторичных» клиентов. Это количество нельзя увеличить иначе, чем перенеся нужное приложение на серверную платформу.

2.2. Подготовка к установке

2.2.1. Соответствие системным требованиям

Прежде чем начинать установку операционной системы на компьютер-клиент, вы должны подготовить всю информацию, которая вам потребуется во время установки. Необходимо также, чтобы оборудование компьютера соответствовало нижеприведенным системным требованиям.

Тип и быстродействие процессора

Для установки операционной системы Windows XP Professional необходим как минимум процессор Pentium II 233 МГц (рекомендуется 300 МГц). Windows 2000 Professional требует хотя бы процессора Pentium 133 МГц.

Объем оперативной памяти

Система Windows XP Professional требует 64 Мб RAM (рекомендуется 128 Мб). Система Windows 2000 Professional требует 32 Мб RAM (рекомендуется 64 Мб).

Объем жесткого диска

Для установки системы Windows XP Professional требуется не менее 1.5 Гб свободного места на жестком диске, для установки системы Windows 2000 Professional — не менее 1 Гб. Кроме этого, понадобится место для дополнительных компонентов Windows и для будущих обновлений Service Pack (эти обновления содержат исправления обнаруженных ошибок и добавляют новые возможности).

Совместимость устройств

Какой смысл иметь новейшую видеокарту, если для нее не существует драйвера под установленную у вас операционную систему? Перед установкой ОС следует убедиться в том, что все ваше оборудование с ней совместимо. Список устройств, проверенных на совместимость (HCL, Hardware Compatibility List), вы найдете на `http://www.microsoft.com/hcl`. В этом списке перечислены как отдельные устройства, так и целые модели компьютеров, а для некоторых устройств можно найти также протестированные драйверы.

Если у вас новейшая модель компьютера или какие-то устройства последнего поколения, может случиться, что в приведенном списке вы их не найдете. В этом нет ничего удивительного: тщательное тестирование продолжается определенное время. В этом случае вам придется самостоятельно искать необходимый драйвер (обычно его находят на сайте производителя устройства) и устанавливать его вручную.

Примечание редактора.

На клиентский компьютер можно рискнуть установить и непроверенный драйвер. Худшее, чем это грозит, — это неправильная или нестабильная работа устройства, что для рабочей станции не слишком критично.

Вместительность диска

О минимальном необходимом свободном месте на диске речь уже шла выше. Каков же должен быть максимальный размер диска?

Обычной практикой является размещение всех пользовательских данных на серверах. Это выгодно как с точки зрения безопасности, потому что серверы обычно хорошо защищены, так и с точки зрения мобильности пользователей: эти данные доступны с любого компьютера в сети. Диск клиентской рабочей станции должен вмещать только операционную систему, приложения, с которыми работает пользователь, и, может быть, локальные данные. Необходимо предупредить пользователей о том, что за сохранность локальных данных отвечает только сам пользователь и в случае какого-либо сбоя администратор восстанавливать их не будет.

Если эти данные пользователю необходимы, он должен сам выполнять их резервное копирование на съемные носители.

Осталось заметить только, что разумнее всего использовать уже проверенные временем марки и модели жестких дисков.

Физическая и логическая структура диска

В подавляющем большинстве случаев на рабочей станции для текущей работы хватает одного физического диска. Исключение составляют те случаи, когда пользователь нуждается в высокой производительности дисковой подсистемы (например, когда компьютер используется для обработки графики) или когда на станции организован массив RAID с целью повышения надежности и/или быстродействия.

Логическая структура диска определяет, будет ли доступен пользователю только один раздел C: или несколько разделов. На рабочей станции вполне достаточно одного раздела. Аргумент о необходимости логически отделить операционную систему от данных здесь не работает, потому что данные (папка **Мои документы**) хранятся на сервере. Более того, некоторых пользователей наличие нескольких разделов просто собьет с толку.

Примечание редактора.

Тем не менее самой распространенной структурой жесткого диска остаются два раздела C: и D:. В разделе C: объемом 10 Гб размещаются операционная система и стандартные приложения: Microsoft Office, архиваторы, файловые менеджеры. В раздел D:, занимающий остальной объем физического диска, устанавливают приложения, требовательные к дисковому объему и монопольному доступу, а также установочные файлы, драйверы и не очень важные документы. Например, программу Adobe Photoshop не рекомендуется устанавливать в раздел, где размещен файл подкачки, то есть в системный раздел.

2.2.2. Файловая система

Во время установки операционной системы вам будет необходимо отформатировать жесткий диск какой-либо из файловых систем: FAT, FAT32 или NTFS. Сейчас мы обсудим, чем следует руководствоваться при выборе файловой системы.

Назначение компьютера

Если на компьютере предполагается установка нескольких операционных систем (такая конфигурация называется multi-boot, или система с вариантами загрузки), то для раздела с данными, доступ к которым необходимо обеспечить из каждой операционной системы, следует выбрать такую

файловую систему, которую «понимают» они все. Сами же операционные системы должны быть установлены в разделы с «родными» для них файловыми системами. Так, MS DOS можно установить только на FAT16, но не на FAT32 или NTFS.

Количество и объемы жестких дисков

Вместе с повышением вместимости диска ограничивается возможность выбора файловой системы. Например, разделы, превышающие в объеме 32 Гб, нельзя форматировать ни в какой другой файловой системе, кроме NTFS. Windows XP Professional и Windows 2000 Professional умеют работать с разделами FAT32, превышающими 32 Гб, но не умеют их создавать. Если вам все-таки нужен раздел FAT32 больший 32 Гб, загрузитесь с загрузочного диска Windows 98 или Windows Millennium Edition и воспользуйтесь утилитой **Format**, находящейся на этом диске.

Требования безопасности

Единственной файловой системой, которая способна защитить файлы или папки на жестком диске от несанкционированного доступа, является NTFS. Ни одна из систем FAT такой способностью не обладает.

Дополнительные требования к файловой системе

Если вам нужны такие возможности, как дисковые квоты, сжатие или шифрование данных, символьные ссылки на папки (Junction Points), то выбирать следует только NTFS.

Характеристики файловых систем, которые также могут послужить основанием для выбора одной из них, приведены в таблице 2.1.

Ограничения файловых систем в Windows XP Professional и Windows 2000 Professional *Таблица 2.1*

	NTFS	FAT32	FAT16
Максимальный размер файла	Теоретически: 16 экзабайт (2^{64}байт) минус 1 Кб; практически: 16 терабайт (2^{44} байт) минус 64 Кб	4 Гб (2^{32} байт) минус 1 байт	4 Гб (2^{32} байт) минус 1 байт
Максимальный размер раздела	Теоретически: 2^{64} кластера минус 1 кластер; практически: 2^{32} кластера минус 1 кластер (256 терабайт минус 64 Кб)	Практически: 32 Гб	4 Гб
Количество файлов в разделе	4 294 967 295 (2^{32} минус 1 файл)	4 177 920	Приблизительно 65 536
Максимальное количество файлов и подпапок в папке	Не ограничено	65 534 (при использовании длинных имен — еще меньше)	512 (при использовании длинных имен — еще меньше)

Из приведенных данных следует, что, если в компьютер будет установлена только Windows XP Professional (или Windows 2000 Professional), будет уместно отформатировать диск файловой системой NTFS.

2.2.3. Необходимые сведения

Перед началом установки подготовьте следующую информацию:

- **Имя пользователя и название организации, на которую зарегистрирован продукт**. Эти данные будут отображаться в окне программы Сведения о системе. Впоследствии их можно будет изменить правкой системного реестра.

Примечание.

При установке Windows XP Professional нельзя в качестве имени пользователя указывать имя Administrator (Администратор).

- **Код Product Key (его, как правило, можно найти на обратной стороне коробки от диска CD-ROM)**. Если вы будете проводить установку с носителя информации, полученного по программе оптового лицензирования корпорации Microsoft, получите этот код от поставщика программных продуктов вашей организации.
- **Имя компьютера.** Оно должно быть уникальным в пределах сети. Правильнее образовывать имена компьютеров не от имен их пользователей, а от назначения, расположения или административной принадлежности самих рабочих станций.
- **Пароль локального администратора (пользователь Administrator или Администратор).** Одна из этих двух учетных записей создается в процессе установки системы. Поскольку эта учетная запись получает привилегии администратора, ее пароль должен отвечать требованиям безопасности.
- **Название рабочей группы, в которую будет включен компьютер.**

Собрав всю эту информацию, вы можете приступать к установке операционной системы Windows XP Professional согласно дальнейшим инстукциям.

Примечание редактора.

Как и в случае с серверной ОС, надежнее будет ставить нелокализованную (английскую) версию операционной системы, а поверх нее — пакет MUI (Multilingual User Interface) для русификации.

2.3. Установка с компакт-диска

Этот параграф содержит подробную последовательность установки, включая диалоговые окна и дополнительные изображения. Для успешной установки вам потребуются загрузочный компакт-диск с операционной системой Windows XP Professional и «чистый» компьютер.

1. В системе BIOS (базовая система ввода-вывода) компьютера необходимо настроить следующую последовательность загрузки с устройств:
   - CD-ROM.
   - Жесткий диск.

   Эта настройка всегда зависит от типа BIOS, поэтому ее нельзя описать универсально. Подробную информацию вы найдете в описании, прилагающемся к вашей материнской плате.
2. В привод CD-ROM вставьте установочный компакт-диск с операционной системой Windows XP Professional и перезагрузите компьютер.
3. Установка системы должна начаться автоматически. Если этого не происходит, проверьте еще раз порядок загрузки в BIOS. Если же в компьютере уже была установлена какая-то операционная система, может случиться так, что для начала установки системе будет требоваться нажатие любой клавиши.
4. Включится текстовый режим установки и появляется окно с надписью **Windows XP Professional Setup (Установка Windows XP Professional)**.
5. Когда на экране появится надпись **Setup Welcome (Вас приветствует программа установки)**, нажмите клавишу **Enter**.

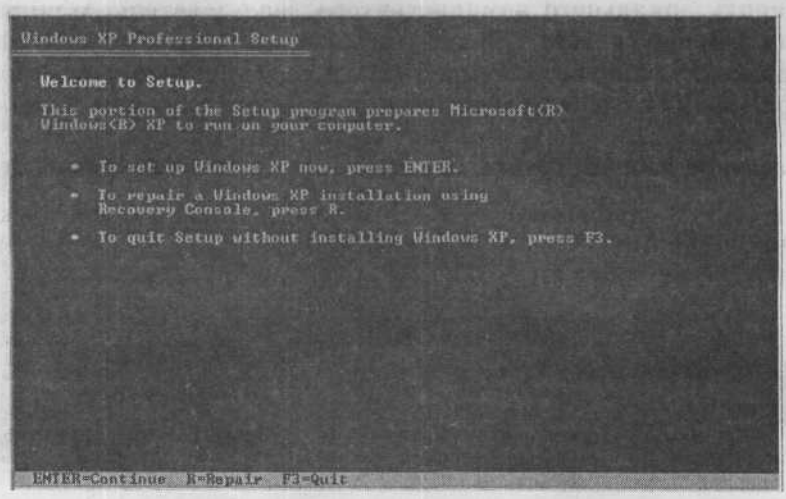


Рис. 2.1. *Диалоговое окно Установочная программа системы Windows XP Professional*

6. После появления надписи **Licensing Agreement (Лицензионное соглашение операционной системы Windows XP)** (см. рис. 2.2) подтвердите нажатием клавиши **F8** согласие с условиями лицензии.

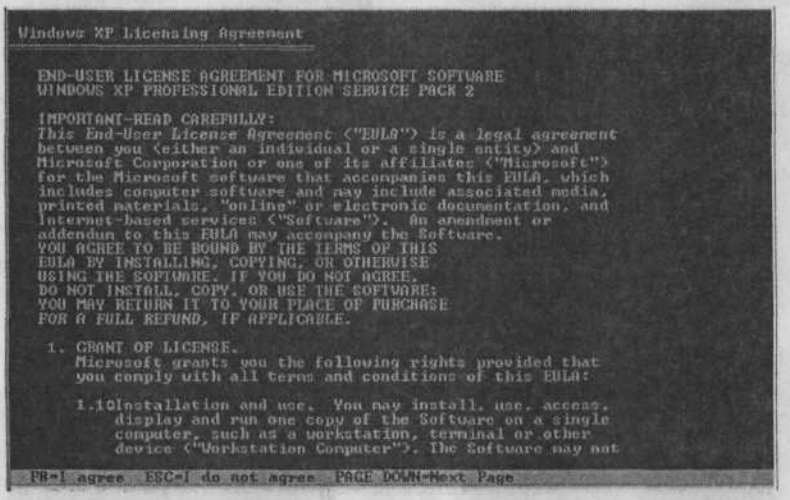


Рис. 2.2. *Лицензионное соглашение операционной системы Windows XP*

7. В следующем окне нужно создать (или изменить) логическую структуру жесткого диска. Нажмите клавишу **C**, что позволит вам создать раздел для установки операционной системы.

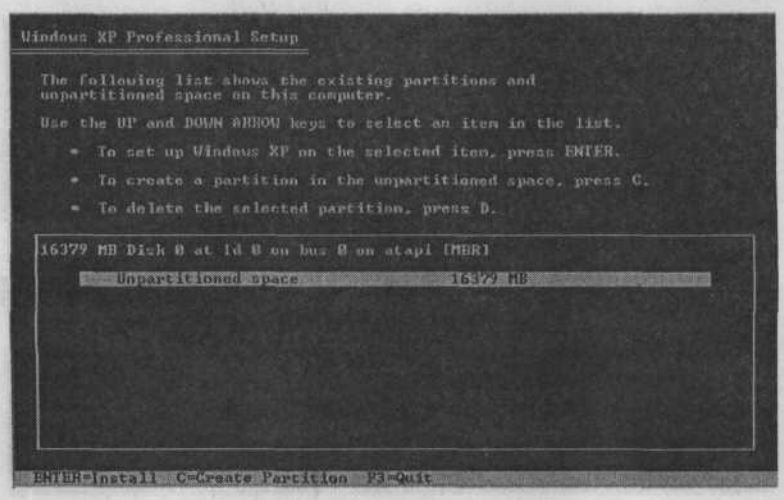


Рис. 2.3. *Создание раздела на жестком диске во время установки*

8. В части **Create a Partition (Создать раздел объёма)** отображен максимально доступный объем жесткого диска. Для системного раздела C: отведите 10240 Мб (то есть 10 Гб). Остальное место отведите под диск D:.

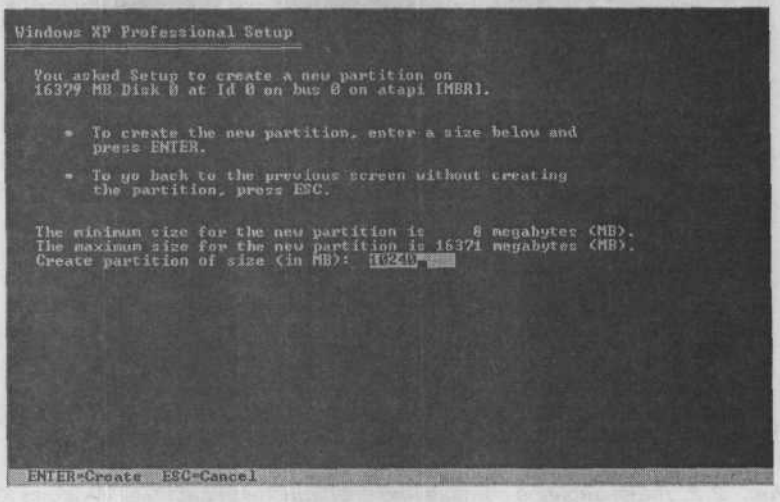


Рис. 2.4. *Определение размера созданного раздела на жестком диске*

9. В списке разделов вновь созданный раздел должен быть обозначен как раздел C:. Если это не так, назначьте ему букву C: и нажмите клавишу **Enter**.

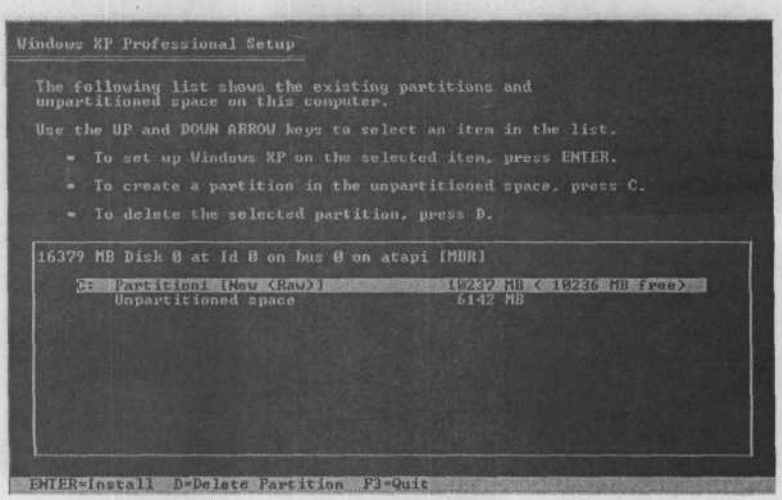


Рис. 2.5. *Раздел, в который произойдет установка Windows XP Professional*

10. В следующем диалоговом окне вы можете выбрать файловую систему, которую следует создать на новом разделе. Если вы не сомневаетесь в качестве поверхности диска, установите переключатель в положение **Format in NTFS File System (Quick) (Отформатировать раздел файловой системой NTFS (Быстро))** — так вы сэкономите время. Если у вас есть сомнения, выберите положение **Format in NTFS File System (Отформатировать раздел файловой системой NTFS)**. В этом случае при форматировании будет произведен физический контроль поверхности и поврежденные («bad») блоки будут исключены из использования. После форматирования раздела начнется копирование файлов в установочную папку Windows XP Professional.

Примечание.

Если вы устанавливаете не XP, а Windows 2000 Professional, то возможность быстрого форматирования будет недоступна.

11. После копирования файлов будет произведена перезагрузка, и установка будет продолжена в графическом режиме.

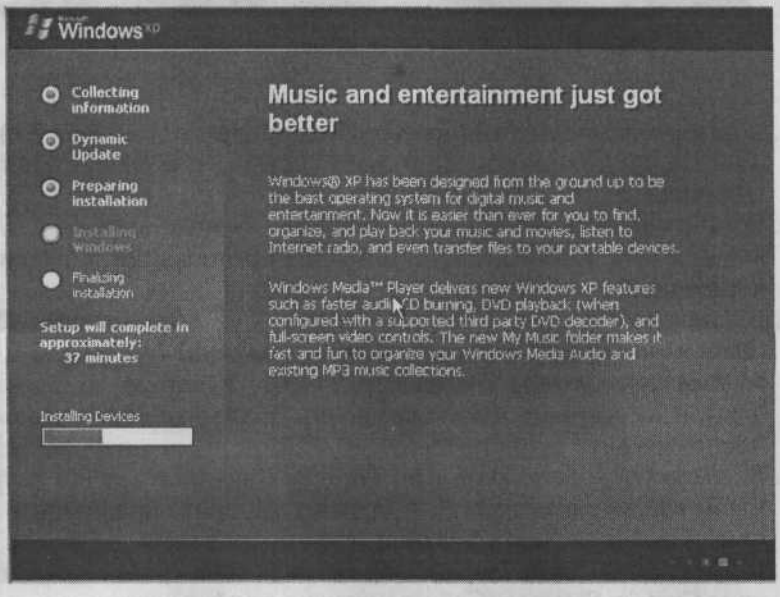


Рис. 2.6. *Графический режим установки операционной системы Windows XP Professional*

12. В диалоговом окне **Regional and Language Options (Региональные и языковые настройки)** (см. рис. 2.7) выберите подходящие региональные настройки (язык, формат дат и времени, денежные единицы) и раскладку клавиатуры и нажмите кнопку **Next (Дальше)**.

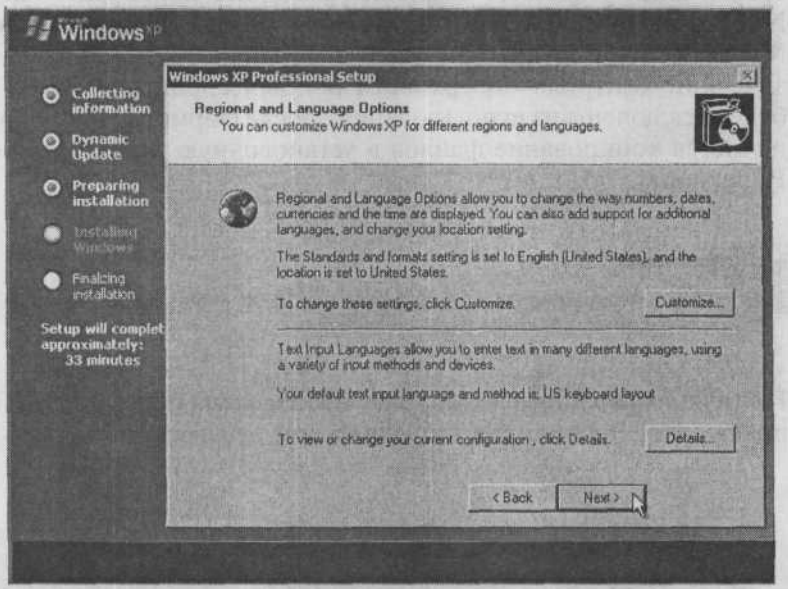


Рис. 2.7. *Окно региональных и языковых настроек*

13. В диалоговом окне **Product Key (Код продукта)** (см. рис. 2.8) введите код для установки операционной системы и нажмите кнопку **Next (Дальше)**.
14. В диалоговом окне **Personalize software (Личные данные)** (см. рис. 2.9) введите имя пользователя и название организации, которая купила лицензию.
15. В диалоговом окне **Computer Name And Administrator Password (Имя компьютера и пароль администратора)** (см. рис. 2.10) введите имя компьютера (например, PC001) и пароль администратора длиной не меньше шести символов. Нажмите **Next (Дальше)** для продолжения.
16. В диалоговом окне **Date And Time Settings (Настройка даты и времени)** введите текущую дату, время и выберите правильный часовой пояс. Нажмите **Next (Дальше)** для продолжения.
17. В диалоговом окне **Networking Settings (Настройка сети)** отметьте поле **Custom Settings (Собственные настройки)** и нажмите на кнопку **Next (Дальше)**.

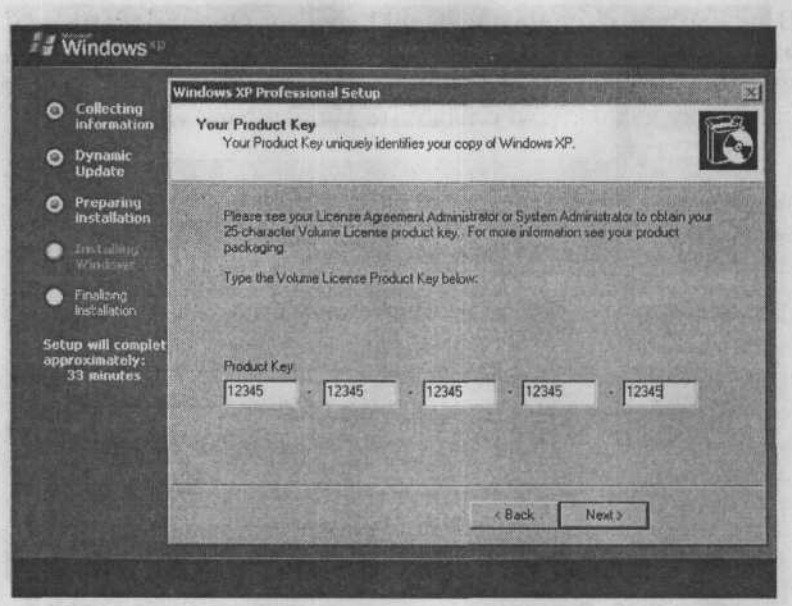


Рис. 2.8. *Ввод кода Product Key*

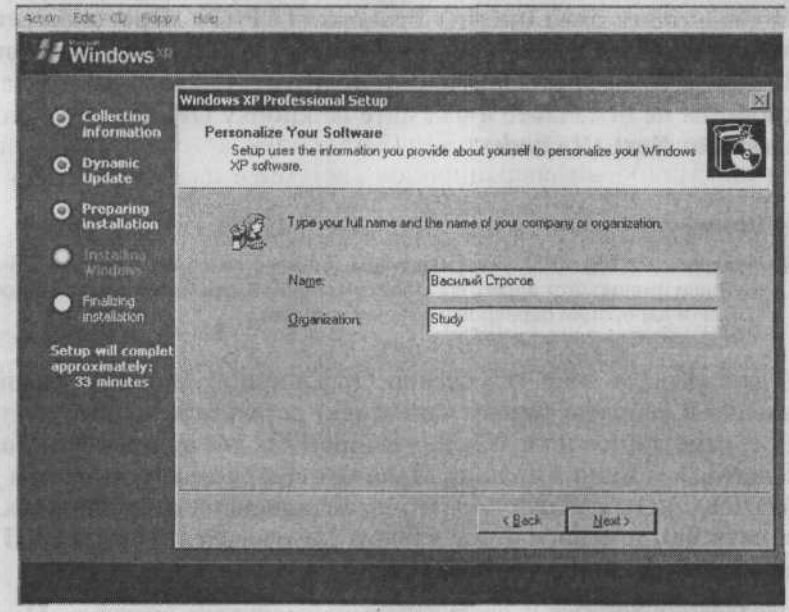


Рис. 2.9. *Окно ввода личных данных*

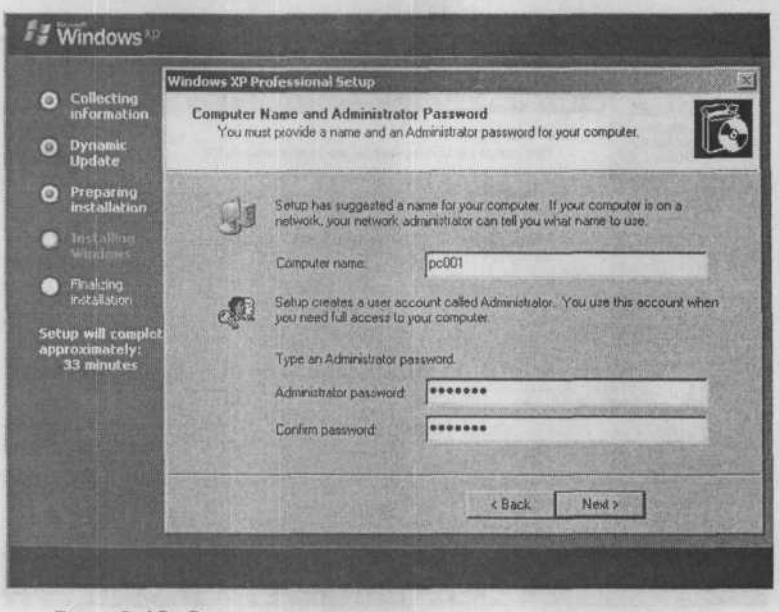


Рис. 2.10. *Окно ввода компьютера и пароля администратора*

18. В диалоговом окне **Networking Components (Настройки сети)** выберите строку **Internet Protocol (TCP/IP) (Протокол сети Интернет (TCP/IP))**, а затем нажмите на кнопку **Properties (Свойства)**.
19. В диалоговом окне **Internet Protocol (TCP/IP) (Протокол сети Интернет (TCP/IP)) — Properties (Свойства)** (см. рис. 2.11) введите IP-адрес 192.168.10.17 и маску подсети 255.255.255.0. Остальные свойства не отмечайте и нажмите на кнопку **OK**. Для продолжения нажмите **Next (Дальше)**.

Примечание.

IP-адрес 192.168.10.17 мы предлагаем только в качестве примера. Почему мы выбрали именно этот адрес, вы узнаете из главы 3, где мы расскажем о протоколе TCP/IP и адресации серверов и рабочих станций.

20. В диалоговом окне **Workgroup Or Computer Domain (Компьютер входит в рабочую группу или домен)** оставьте исходные настройки (т.е. отмеченное поле **No, this computer is not on a network, or is on a network without a domain. Make this computer a member of a group: WORKGROUP — Компьютер не подключен к сети или подключен к сети без домена и будет членом следующей группы ГРУППА**) и нажмите на кнопку **Next (Дальше)**.

После задания этих параметров начнется установка системы. По завершении установки компьютер будет перезагружен.

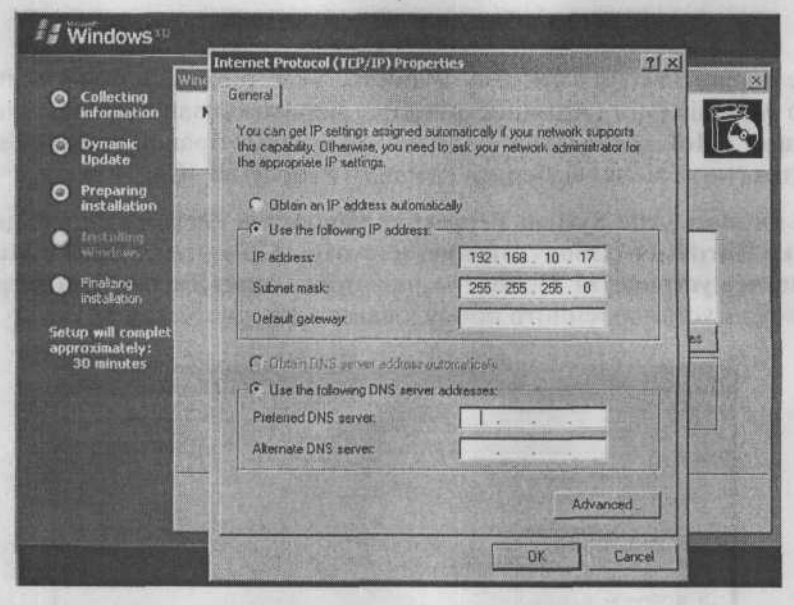


Рис. 2.11. *Настройка протокола IP*

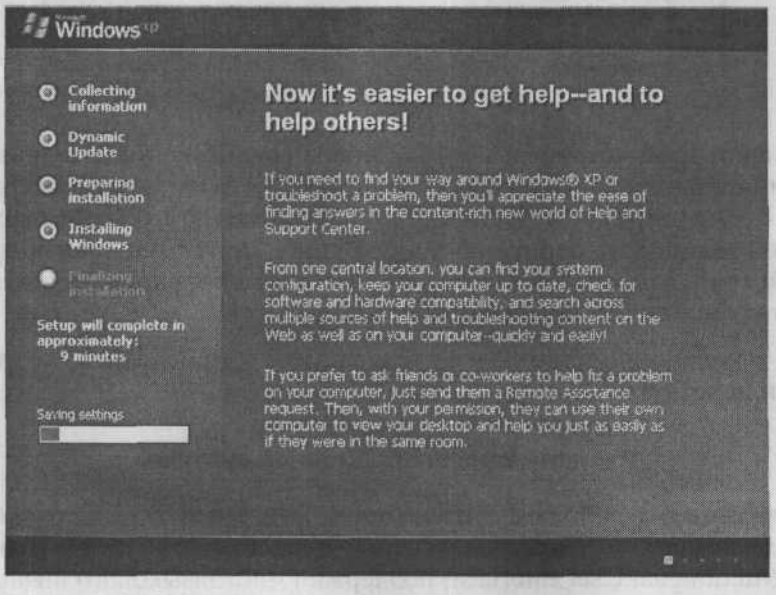


Рис. 2.12. *Последний этап установки операционной системы Windows XP Professional*

Установка драйверов устройств

После первого входа в систему Windows XP Professional под учетной записью Administrator (Администратор) выберите в главном меню пункт **My Computer (Мой компьютер)** и щелкните по нему правой кнопкой мыши. В контекстном меню выберите команду **Properties (Свойства)**.

В диалоговом окне **System Properties (Свойства системы)** перейдите на вкладку **Hardware (Оборудование)** и нажмите на кнопку **Device Manager (Диспетчер устройств)**. Появится диалоговое окно **Диспетчера устройств** со списком установленного оборудования (см. рис. 2.13).

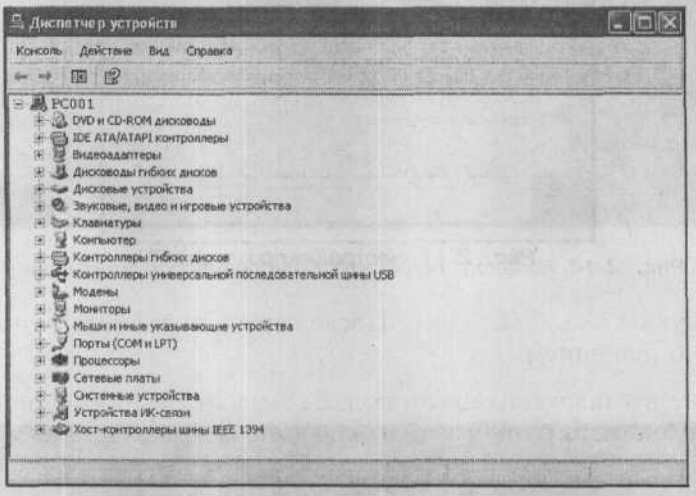


Рис. 2.13. *Список установленного оборудования*

Если некоторые устройства будут отображены с вопросительным или восклицательным знаком, значит, в системе не было подходящего драйвера к этому устройству. Нажмите по очереди на эти устройства правой кнопкой мыши и выберите команду **Update Driver (Обновить драйвер устройства)**. Запустится Мастер обновления оборудования, которому нужно предоставить правильный драйвер.

После правильной установки драйвера знак вопроса около устройства должен исчезнуть.

Русификация операционной системы

Для того, чтобы работать в привычной нам среде с русскоязычными командами меню и диалоговыми окнами, необходимо установить пакет MUI (Multilingual User Interface) поддержки многоязыкового интерфейса. Запустите программу установки, обычно расположенную в папке MUI и

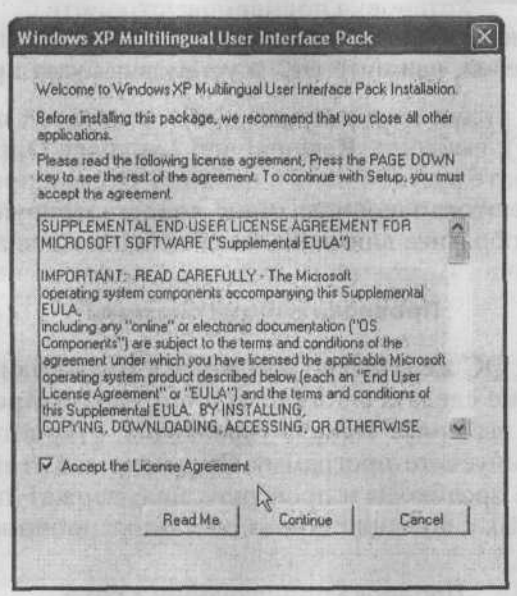


Рис. 2.14. *Начало установки MUI. Лицензионное соглашение*

называющуюся `muisetup.exe`. После запуска появится окно с лицензионным соглашением.

Нужно отметить галочкой свое согласие с условиями и нажать **Continue (Продолжить)**. После этого отобразится окно выбора языков (см. рис. 2.15).

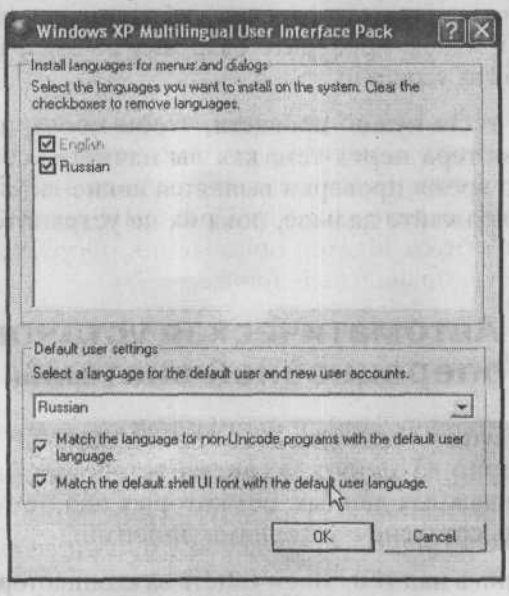


Рис. 2.15. *Выбор языков*

Выберите из списка язык по умолчанию для всех будущих учетных записей пользователей, нажмите **OK**, и установка будет произведена.

Чтобы включить русскоязычный интерфейс, откройте **Control Panel** (**Панель управления**), выберите **Regional and Language Options**, на вкладке **Languages** выберите русский язык и нажмите **OK** для применения новых установок. После этого закончите сеанс и зарегистрируйтесь снова. При входе в систему обратите внимание на раскладку клавиатуры.

Проверка работы системы

После установки ОС желательно убедиться в том, что она работает правильно. Это можно сделать с помощью инструмента **Просмотр событий**. В главном меню выберите **Панель управления**, откройте окно **Администрирование** и запустите программу **Просмотр событий**. Просмотрите все приведенные протоколы и проверьте, не содержат ли они серьезных ошибок, связанных с функционированием операционной системы.

Проверка подключения к сети

В главном меню выберите пункт **Выполнить** и в поле **Открыть** окна **Запуск программы** введите команду CMD. Появится окно командной строки Windows XP Professional. В командной строке введите команду PING и IP-адрес сервера, установленного в предыдущей главе (PING 192.168.10.2). Если проверка пройдет успешно (вы увидите, что ваш компьютер получает ответы от сервера), обратитесь к серверу по имени (PING SRVR001), чтобы проверить разрешение имен в сети. Этот тест тоже должен пройти успешно.

Эти три простых теста нужно провести, чтобы проверить правильность настройки компьютера перед тем, как вы начнете устанавливать приложения. Если во время проверки выявятся какие-либо ошибки или неточности, не продолжайте дальше, пока их не устраните.

2.4. Автоматическая установка операционной системы

Допустим, предыдущая установка системы Windows XP Professional продолжалась примерно 45 минут. Во время установки было необходимо ввести несколько важных данных, без которых она не могла бы продолжаться: например, согласие с условиями лицензии.

Вы уже задумывались над тем, зачем сидеть за компьютером и ждать, если чистое время вашего взаимодействия с Мастером установки — считанные

минуты? Может быть, можно заранее записать ответы и предоставить их Мастеру установки?

При установке ОС Windows XP Professional и Windows 2000 Professional это сделать можно. Все вводимые данные нужно записать в так называемый файл ответов и передать его программе установки как параметр. После этого можно отойти от компьютера и заняться чем-нибудь не менее полезным, а установка пойдет без вашего участия.

Файл ответов имеет точно определенный формат. Он состоит из разделов, ключей и их параметров. Примерный файл ответов, содержащий все допустимые разделы, ключи и возможные параметры, находится на дистрибутивном компакт-диске. Создать собственный файл ответов на основе примерного — задача не самая простая, и корпорация Microsoft предлагает для этой цели утилиту **Диспетчер установки**.

Примечание редактора.

К сожалению, на купленных на лотках дистрибутивах, которыми пользуются многие из нас, копии файла ответов есть далеко не всегда.

Подготовка файла ответов

Файл ответов можно подготовить на любом компьютере, не обязательно на том, где уже установлена Windows XP Professional. Действуйте в следующем порядке:

1. На диске C: создайте папку DEPLOY.
2. Вставьте в привод CD-ROM дистрибутивный диск с операционной системой Windows XP Professional. Перейдите к папке `Support\tools` и откройте архив DEPLOY (точнее, DEPLOY.CAB, но в ваших текущих настройках папки стандартные расширения могут оказаться скрыты). Появится его содержимое — всего 10 файлов.

Примечание.

Чтобы отображать все расширения, в окне **Проводника** выполните команду Сервис → Свойства папки и на вкладке **Вид** снимите флажок **Скрывать расширения для зарегистрированных типов файлов**.

3. Нажатием комбинации клавиш Ctrl+A выделите все 10 файлов и выполните команду **Файла → Извлечь**.
4. В качестве места назначения укажите папку C:\DEPLOY, созданную на первом шаге.
5. Нажмите кнопку **Извлечь**.

6. Запустите программу `C:\DEPLOY\Setupmgr.exe`. Это Мастер установки Windows, на первом шаге которого запускается Диспетчер установки, помогающий подготовить файл ответов. Запустите Диспетчер, нажав кнопку **Далее**.
7. В диалоговом окне **Новый или существующий файл ответов** установите переключатель в положение **Создать новый файл ответов** и нажмите **Далее**.
8. В диалоговом окне **Тип установки** выберите **Автоматическая установка** и нажмите **Далее**.
9. В диалоговом окне **Продукт** выберите **Windows XP Professional** и нажмите **Далее**.
10. В диалоговом окне **Взаимодействие с пользователем** (рис. 2.16) выберите **Полностью автоматическая установка** и нажмите **Далее**.

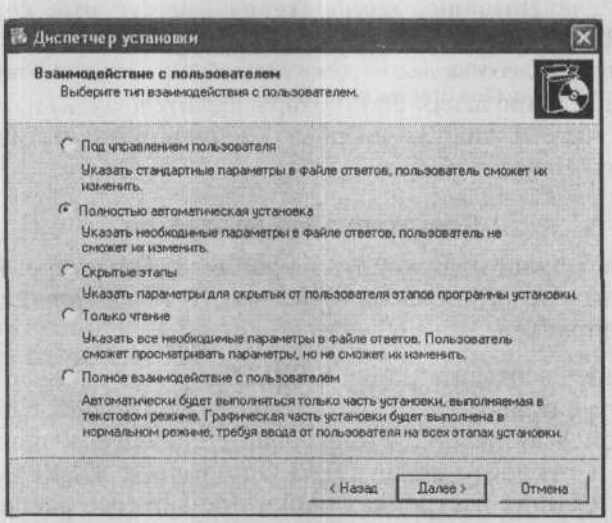


Рис. 2.16. *Диалоговое окно* ***Взаимодействие с пользователем***

11. В диалоговом окне **Дистрибутивный общий ресурс** выберите **Установить с компакт-диска** и нажмите **Далее**.
12. Приступайте к вводу ответов. В диалоговом окне **Лицензионное соглашение** отметьте поле **Соглашаюсь с условиями лицензионного соглашения** и нажмите **Далее**. Этот ответ имитирует нажатие клавиши F8 в ходе интерактивной установки.
13. В разделе **Установка программного обеспечения** введите имя пользователя и название организации, которая приобрела лицензию. Нажмите **Далее**.

Примечание.

Имя пользователя Администратор задавать нельзя. Система Windows XP Professional не узнает этого имени, и автоматическая установка остановится.

14. В разделе **Параметры экрана** задайте цветовую палитру, область экрана и частоту обновления монитора компьютера назначения. Внимание: для того, чтобы эта настройка работала, у Мастера установки операционной системы Windows XP Professional должен быть драйвер для видеоадаптера компьютера назначения. Нажмите **Далее**.
15. В разделе **Часовой пояс** задайте свой часовой пояс и нажмите **Далее**.
16. В разделе **Ключ продукта Product Key** введите код Product Key с обратной стороны футляра дистрибутивного компакт-диска и нажмите **Далее**.
17. В разделе **Названия компьютеров** введите имя компьютера назначения (PC002) и нажмите кнопку **Присвоить**. Для продолжения нажмите **Далее**.
18. В разделе **Пароль администратора** введите дважды пароль (4e4etk@) и включите опцию **Зашифровать пароль администратора в файле ответов**. Нажмите **Далее**.
19. В разделе **Сетевые компоненты** установите переключатель в положение **Особые параметры**, выберите пункт **Протокол сети Интернет (TCP/IP)** и нажмите кнопку **Свойства**. Включите опцию **Использовать адрес IP** и введите адрес 192.168.10.18 и маску подсети 255.255.255.0. Остальные значения оставьте как есть. Нажатием кнопки **OK** закройте диалоговое окно **Свойства протокола сети Интернет (TCP/IP)**. Для продолжения нажмите **Далее**.
20. В разделе **Рабочая группа или домен** оставьте исходные настройки с названием **Группа** и нажмите **Далее**.
21. В разделе **Телефония** оставьте исходные настройки и нажмите **Далее**.
22. В разделе **Язык и стандарты** оставьте исходные настройки и нажмите **Далее**.
23. В разделе **Языки** выберите **Cyrillic (Кириллические)** и нажмите **Далее**.
24. В разделе **Параметры обозревателя и оболочки** введите параметры, соответствующие вашей рабочей среде (здесь можно задать настройки для прокси-сервера).
25. В разделе **Инсталляционная папка** включите опцию **В папку с указанным именем** и введите имя папки Windows. Таким образом вы обеспечите совместимость с ранее установленными компьютерами.
26. В разделе **Устанавливаемые принтеры** нажмите **Далее**.
27. В разделе **Однократное выполнение** нажмите **Далее**.
28. В разделе **Дополнительные команды** нажмите кнопку **Закончить** и в диалоговом окне **Мастер установки Windows** укажите путь к

папке, в которой будет создан файл ответов. Можно оставить путь по умолчанию `C:\DEPLOY\unattend.txt`. Нажмите **OK**.

29. Теперь файл создан. Закройте **Мастер установки** нажатием крестика в правом верхнем углу окна.

Откройте файл `C:\DEPLOY\unattend.txt` и просмотрите список сгенерированных разделов, ключей и их параметров. Если вы найдете опечатку или другую неточность, исправьте ее прямо в файле. Встретив опечатку, программа установки остановится и будет ожидать ввода правильного параметра. Вместе с файлом `unattend.txt` будет создан также файл `unattend.bat`. Он не понадобится, и можете удалить его с чистой совестью.

Примечание.

В Windows 2000 Professional файл ответов генерируется аналогично, с той лишь разницей, что он не содержит кода Product Key, который нужно вводить вручную. Если вы хотите, чтобы установка была полностью автоматической, необходимо отредактировать файл ответов следующим образом: в раздел `[UserData]`, содержащий имя пользователя и названия организации и компьютера, добавьте пункт ProductID=12345-12345-12345-12345-12345(разумеется, этот код — только пример).

Примечание.

Полный список всех разделов, ключей и параметров вы найдете в файле `Deploy.chm` в разделе `Ссылка`.

Установка с помощью файла ответов

В предыдущем разделе мы создали файл ответов, которого вполне достаточно для полной автоматической установки Windows XP Professional на один компьютер. Остается вопрос: как «скормить» этот файл программе установки, если, как вы могли убедиться в ходе интерактивной установки, прерывать и возобновлять ее работу нельзя?

Очевидно, что загрузочная дискета (которую в случае Windows XP Professional нужно скачать из Интернета) здесь не поможет: она применяется только для загрузки системы в том случае, если BIOS не поддерживает загрузку с CD-ROM. После загрузки программа-инсталлятор запускается с компакт-диска обычным способом.

Для успеха задуманной операции нужно знать небольшой трюк:

1. В настройках BIOS компьютера назначения укажите следующий порядок загрузочных устройств:

- CD-ROM.
- Жесткий диск.
- Дискета.

2. Файл `unattend.txt` переименуйте в WINNT.SIF и запишите его на пустую (не загрузочную) дискету. Можно использовать и дискету, уже содержащую файлы или папки, но тогда обязательно поместите файл WINNT.SIF в ее корневой каталог, то есть A:\WINNT.SIF.
3. Вставьте дискету в дисковод для гибких дисков, а в привод CD-ROM вставьте загрузочный диск дистрибутива Windows XP Professional и перезагрузите компьютер.

При загрузке компьютера с компакт-диска программа установки «заглядывает» во флоппи-дисковод, проверяя, есть ли там дискета, а на дискете — файл WINNT.SIF. Если есть, то она прочитывает этот файл и руководствуется им. Если нет, то она начинает обычную интерактивную установку системы.

После окончания установки выньте дискету из дисковода.

2.5. Установка в крупной сети

Если вы внимательно следили за порядком автоматической установки операционной системы Windows XP Professional, то заметили, что файл ответов предназначен только для одного компьютера (включает уникальные параметры, такие как имя компьютера, код Product Key или IP-адрес). Так возможна ли автоматическая установка на все клиентские компьютеры сети?

Конечно, единственным решением будет подготовить отдельный файл ответов для каждой рабочей станции. Однако в крупной сети это станет большой проблемой и возможным источником ошибок, которые проявятся в самый неподходящий момент — во время установки. Давайте посмотрим на уникальные параметры подробнее.

Код Product Key

Если вы проводите автоматическую установку «коробочных» версий операционной системы Windows XP Professional, обязательно убедитесь, что каждый компьютер имеет уникальный код Product Key. В противном случае не позднее чем через 30 дней после установки вы столкнетесь с трудностями при активации продукта. В этом случае код Product Key нужно принимать за уникальный параметр.

Если вы получили операционную систему Windows XP Professional по одной из программ оптового лицензирования корпорации Microsoft, вы

должны иметь единый универсальный код Product Key. В этом случае код пригоден для всех компьютеров и не является уникальным параметром.

Имя компьютера

Очевидно, что имя компьютера в сети — это всегда уникальный параметр. При автоматической установке нужно тщательно следить за тем, чтобы имена компьютеров не совпали.

IP-адрес

Как и имя, IP-адрес компьютера должен быть уникален в пределах сети. Исключение составляет случай, когда компьютеры уже во время установки получают IP-адрес от сервера DHCP.

Прочие параметры

Есть и другие параметры, которые могут отличаться у разных компьютеров.

Например, IP-адреса серверов DNS, настройки прокси-сервера для приложения Internet Explorer, настройки разрешения экрана, цветовой палитры или горизонтальной частоты обновления монитора и другие. К назначению этих параметров в файле ответов тоже нужно отнестись со всем вниманием.

Как можно предусмотреть все это при автоматической установке? Ответом является файл UDF (Uniqueness Database File).

UDF — файл уникальных параметров

Внимание! Этот способ нельзя использовать при автоматической установке с дистрибутивного компакт-диска. Он годится только для установки по сети или вообще там, где можно запустить программу-инсталлятор из командной строки, передав ей параметры.

1. Создайте в сети отдельную папку для установочных файлов системы Windows XP Professional. В эту папку поместите содержимое папки i386 с дистрибутивного компакт-диска. Компьютеры с такой папкой называются дистрибутивными серверами.
2. Загрузите компьютер назначения с загрузочной дискеты MS DOS.
3. Создайте на компьютере назначения раздел размером не менее 1 Гб и отформатируйте его.
4. Запустите на компьютере назначения сетевой клиент для MS DOS и подключитесь к сетевой дистрибутивной папке с помощью команды net use.

Примечание.

Сетевой клиент для MS DOS можно найти на дистрибутивном компакт-диске с системой Windows NT 4.0 Server.

Теперь можно запустить программу установки с двумя параметрами. Первый — это имя файла ответов, содержащего параметры, одинаковые для всех компьютеров сети, а второй (необязательный) — имя файла базы данных UDF.

Файл UDF имеет такую же структуру, как и файл ответов, но содержит дополнительный раздел `[UniqueIDs]` с уникальными идентификаторами компьютеров, в котором перечислены только те параметры, которые для каждого компьютера отличаются от стандартного набора.

Вот пример файла UDF для двух компьютеров: PC003 и PC004. Они отличаются, естественно, именами и IP-адресами, но PC003 кроме того имеет другую частоту горизонтальной развертки монитора (70Hz) и другую глубину цвета (32 байта).

```
[UniqueIDs]
PC003=UserData,Display,params.MS_TCPIP.Adapter1
PC004=UserData,params.MS_TCPIP.Adapter1
[PC003:UserData]
ComputerName=PC003
[PC003:Display]
Vrefresh=70
BitsPerPel=32
[PC003:params.MS_TCPIP.Adapter1]
IPAddress=192.168.10.19
[PC004:UserData]
ComputerName=PC004
[PC004:params.MS_TCPIP.Adapter1]
IPAddress=192.168.10.20
```

Использовать файл UDF очень просто. В случае установки компьютера PC003 используется вся информация, приведенная в файле ответов, за исключением той, которая для компьютера PC003 определена в файле UDF (или если параметры, приведенные в файле UDF, имеют приоритет по отношению к параметрам в файле ответов).

Пусть файл ответов имеет имя `unattend.txt`, а файл UDF — имя `unattend.udf`, и оба они расположены на дискете. Тогда синтаксис команды запуска установочной программы WINNT.EXE со всеми параметрами для компьютера PC003 будет следующим:

```
WINNT.EXE /u:a:\ unattend.txt / udf:pc003,a:\ unattend.udf
```

При установке компьютера PC004 синтаксис будет очень похожий:

```
WINNT.EXE /u:a:\ unattend.txt / udf:pc004,a:\ unattend.udf
```

Таким образом, для установки, например, 100 компьютеров вам понадобится только два текстовых файла: один с ответами, второй — с исключениями для отдельных компьютеров. При автоматической установке с компакт-диска вам потребовалось бы 100 файлов ответов.

У внимательного читателя мог возникнуть вопрос: если при установке по сети необходимо сначала загрузить компьютер с загрузочной дискеты MS-DOS, потом создать раздел размером хотя бы в 1 Гб (разумеется, с файловой системой FAT) и только потом начинать установку, то не окажется ли после установки, что жесткий диск будет разбит на два раздела C: (1 Гб FAT) и D: (все оставшееся пространство на диске, NTFS)?

Как уже сказано в этой главе, на рабочей станции желательно было бы иметь единственный раздел C:, занимающий весь жесткий диск и отформатированный в файловой системе NTFS. Чтобы получить в итоге установки такой результат, нужно добавить в раздел `[Unattended]` файла ответов две строки:

```
FileSystem=ConvertNTFS
ExtendOEMPartition=1
```

Первая из них конвертирует раздел, созданный DOS, в файловую систему NTFS, вторая расширяет этот раздел на весь физический диск.

2.6. Активация системы

«Коробочную» версию клиентской операционной системы Windows XP Professional после установки необходимо активировать. Активация состоит в проверке того факта, что код продукта (Product Key) данного дистрибутива не использовался на большем количестве компьютеров, чем указано в лицензии.

Если Windows XP Professional устанавливается по программе оптового лицензирования, например Open License или Select License, то активации не требуется: в этом случае для всех рабочих станций организации действителен единый код Product Key.

Систему можно активировать через Интернет (что намного быстрее и проще) или по телефону. Если вы хотите провести автоматическую активацию уже во время установки системы, нужно не забывать о следующем:

1. Во время установки система должна иметь доступ к Интернету. Если для доступа в Интернет вы используете прокси-сервер, необходимо

указать его в файле ответов. Для этого в раздел `[Proxy]` добавьте строки

```
HTTP_Proxy_Server = http://proxyserver:port
Proxy_Enable = 1
Proxy_Override = local,
```

где `proxyserver` — это имя компьютера, выполняющего роль прокси-сервера, а `port` — это номер порта.

2. Файл ответов должен содержать запись, которая обеспечивает автоматическую активацию системы: в раздел `[Unattended]` добавьте строку

```
AutoActive = Yes
```

3. Файл ответов должен содержать ключ `UnattendSwitch`: в раздел `[Unattended]` добавьте строку

```
UnattendedSwitch = Yes
```

Примечание.

Заказ автоматической активации не гарантирует того, что активация действительно произойдет. Помешать этому могут, например, проблемы, возникшие при подключении к Интернету, или неправильная настройка сети.

2.7. Итоги

Клиентом в сети является компьютер, пользующийся услугами серверов. Последовательность установки операционной системы на компьютеры-клиенты очень похожа на последовательность установки ОС на серверы, описанную в предыдущей главе. Благодаря тому, что у компьютеров-клиентов можно предполагать почти одинаковые конфигурации, можно с выгодой использовать автоматическую установку, а там, где это возможно, установку с помощью клонирования дисков.

Если вы хотите использовать автоматическую установку с компакт-диска, дайте файлу ответов имя WINNT.SIF и поместите его в корневой каталог дискеты, которая во время загрузки с компакт-диска должна находиться в дисководе для гибких дисков.

При автоматической установке ОС на несколько компьютеров по сети уместно использовать файл уникальных параметров UDF. Так вы избежите необходимости создавать для каждого компьютера собственный файл ответов. Единственный файл UDF содержит те ключи и параметры, которые для каждого отдельного компьютера отличаются от стандарт-

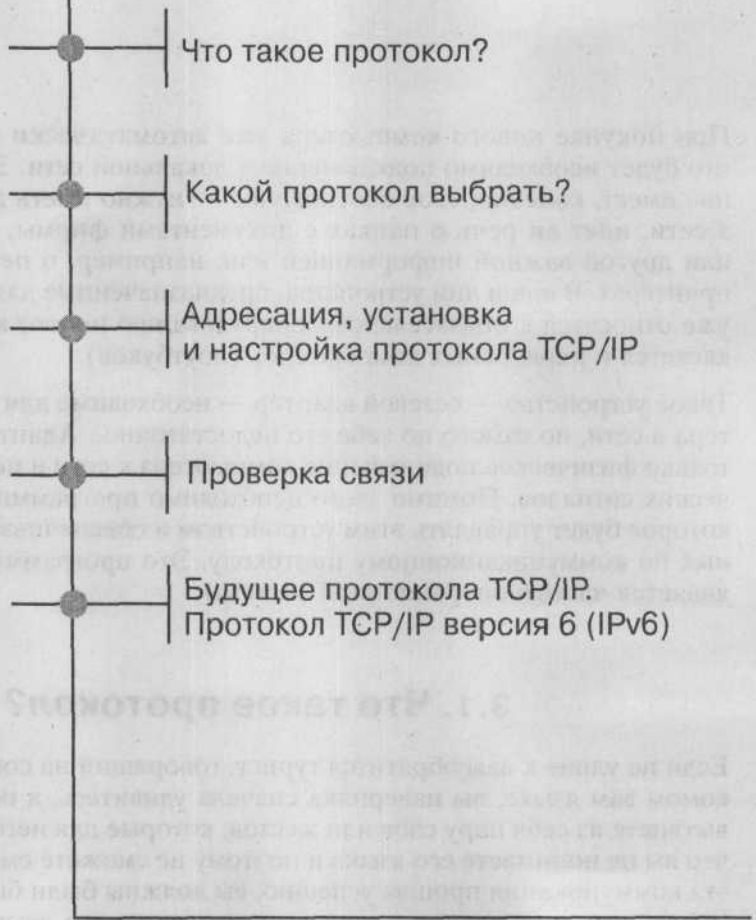
ных, указанных в файле ответов. Во время установки на этот компьютер уникальные ключи имеют приоритет перед стандартными.

До истечения 30 дней после установки операционной системы нужно провести активацию продукта (в случае установки продукта с «коробочной» версии). В противном случае вы не сможете использовать систему.

Состояние сети

Теперь в сети установлены все компьютеры-клиенты, и с помощью утилиты PING проверена связь между ними и сервером.

Глава 3 Учим компьютер работать в сети



При покупке нового компьютера уже автоматически предполагается, что будет необходимо подключение к локальной сети. Это предположение имеет, конечно, свое обоснование — нужно иметь доступ к данным в сети, идет ли речь о папках с документами фирмы, изображениями или другой важной информацией или, например, о печати на сетевых принтерах. В наши дни устройства, предназначенные для коммуникации, уже относятся к обязательному оборудованию нового компьютера. Это касается и переносных компьютеров (ноутбуков).

Такое устройство — сетевой адаптер — необходимо для работы компьютера в сети, но самого по себе его недостаточно.. Адаптер обеспечивает только физическое подключение компьютера к сети и передачу электрических сигналов. Помимо этого необходимо программное обеспечение, которое будет управлять этим устройством и обеспечивать передачу данных по коммуникационному протоколу. Это программное обеспечение является частью операционной системы.

3.1. Что такое протокол?

Если на улице к вам обратится турист, говорящий на совершенно незнакомом вам языке, вы наверняка сначала удивитесь, а потом, возможно, вытянете из себя пару слов или жестов, которые для него будут означать, что вы не понимаете его языка и поэтому не сможете ему помочь. Чтобы эта коммуникация прошла успешно, вы должны были бы, во-первых, понимать его, а во-вторых, уметь выражаться на его языке так, чтобы он понял вас.

Коммуникация компьютеров происходит точно так же. Язык, который компьютеры используют для общения друг с другом, называется коммуникационным протоколом, или просто протоколом. Если два компьютера должны что-то сообщить друг другу и понять друг друга, нужно, чтобы они использовали один и тот же протокол. Таким образом, протокол является еще одной незаменимой частью для успешной коммуникации в сети.

За время, в течение которого развиваются компьютеры и сети, появилось множество коммуникационных протоколов. Некоторые компании включили в свои операционные системы собственные протоколы, другие использовали так называемый открытый протокол. В операционные системы Windows с самого начала было встроено несколько протоколов. Не каждый из них, однако, пригоден для любых условий: для конкретных сетей могут существовать свои ограничения. Первый вопрос при развертывании сети — какой протокол выгоднее всего в ней использовать. При поиске ответа на этот вопрос необходимо учесть следующие моменты:

- Насколько сложна топология сети?
- Сколько компьютеров будет работать в сети?
- Будет ли сеть подключена к Интернету?
- Какие операционные системы будут использоваться в сети?

3.2. Какой протокол выбрать?

В сетевые операционные системы Windows XP Professional и Windows Server 2003 встроено несколько протоколов. Они весьма различны между собой (иначе не было бы смысла включать их все), и не каждый из них можно использовать для одних и тех же целей. Проще говоря, каждый их них подходит для конкретного типа сети.

С первого взгляда может показаться, что самым разумным решением в случае, если вы не уверены, какой протокол лучше подойдет для конкретной сети, будет установить все протоколы и в соответствии с мнением «компьютеру видней» возложить правильный выбор протокола и всю ответственность за связь на компьютер. Но это не выход из положения. Такое решение породит лишние проблемы при устранении трудностей в случае, когда коммуникация в сети не проходила так, как полагается. О перегрузке сети мы даже не говорим.

Прежде чем вы начнете использовать какой-либо протокол, нужно все хорошо обдумать и спланировать. Далее мы подробнее рассмотрим некоторые протоколы операционных систем, начиная с Windows 2000.

3.2.1. NetBEUI

Общее описание

Протокол NetBEUI (NetBIOS Extended User Interface) является очень простым протоколом, который корпорация Microsoft включила в свою первую сетевую операционную систему в 1993 году. В то время существовало не так много компьютерных сетей, и речь всегда шла о локальной сети LAN (Local Area Network). Установка протокола очень быстрая, а функционирование сети стабильно.

Огромным преимуществом использования протокола NetBEUI является возможность использовать его без всякой настройки. Это означает, что после его установки компьютеры сразу же могут начать общение друг с другом — никаких параметров изменять не придется. На заре появления сети это было оптимальным вариантом, так как сеть была тогда совершенно новой технологией и никто не знал, как с ней нужно работать. Более того, протокол NetBEUI устанавливался вместе с Windows как первоначальный протокол, и не было необходимости устанавливать его отдельно.

Последовательность установки протокола NetBEUI в системе Windows XP Professional изменилась по сравнению с предыдущими системами. Вы уже не найдете протокол на «обычном» месте вместе с остальными (рис. 3.1). Поводом к этому послужило изменение типичной сетевой среды: протокол NetBEUI теперь используется редко, значит, нет смысла оставлять его в системе. Он находится на установочном компакт-диске CD-ROM системы Windows XP Professional.

Установка протокола NetBEUI

Последовательность его установки в системе Windows XP Professional следующая:

1. Вставьте в привод установочный компакт-диск с операционной системой Windows XP Professional и перейдите к папке E:\VAULEADD\MSFT\NET\NETBEUI (буквой E: здесь обозначен привод CD ROM, который в вашем компьютере может называться по-другому).
2. Скопируйте файл NBF.SYS в папку %SYSTEMROOT%:\SYSTEM32\DRIVERS, а файл NETNBF.INF — в папку %SYSTEMROOT%\INF.
3. Откройте окно **Подключение к локальной сети — свойства** и нажмите кнопку **Установить**. Теперь среди предлагаемых для установки протоколов будет пункт **Протокол NetBEUI**.

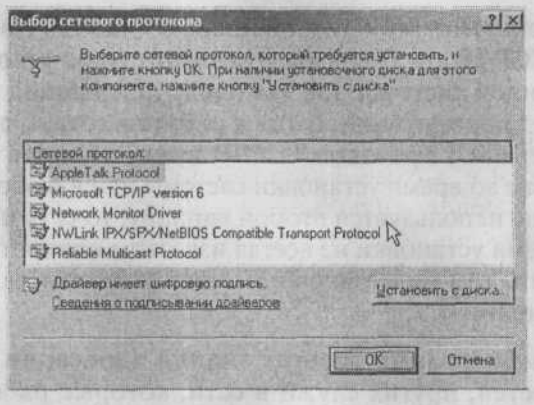


Рис. 3.1. *Протокол NetBEUI среди предложенных протоколов для установки отсутствует*

Примечание.

Если расширения файлов не отображены либо вы не видите папки INF в папке WINDOWS, откройте окно **Мой компьютер** и в меню **Сервис** выберите пункт **Свойства папки**. На вкладке **Вид** снимите флажок **Скрывать расширения для зарегистрированных типов файлов** и установите флажок **Показывать скрытые файлы и папки.**

Существенным недостатком протокола NetBEUI, с современной точки зрения, является то, что он не поддерживает маршрутизацию. Это значит, что в крупной сети (порядка сотни компьютеров) или в сети, объединяющей несколько подсетей, протокол NetBEUI использовать невозможно. Еще более очевидным неудобством отсутствия маршрутизации является невозможность присоединить сеть, основанную на протоколе NetBEUI, к Интернету. Если вы колеблетесь в выборе протокола, то по этим двум причинам лучше отказаться от использования NetBEUI. Его недостатки в наше время значительно перевешивают его достоинства.

3.2.2. TCP/IP

Протокол TCP/IP был создан в 1970 году для пробной сети американского министерства обороны ARPANET, которая позже разрослась до известного сегодня Интернета. Операционные системы UNIX использовали протокол TCP/IP с самого начала. Роль TCP/IP как основного протокола сети Интернет до сих пор является неоспоримым доказательством его надежности и функциональности. Другим его преимуществом является наличие версий для любых компьютерных платформ.

Операционные системы Windows, начиная с Windows 2000, уже используют протокол TCP/IP как базовый. Это значительно ускоряет установку новой операционной системы, так как после завершения установки компьютер сразу, без перезагрузки, готов к работе в сети. Однако в отличие от протокола NetBEUI протокол TCP/IP нужно сконфигурировать. Это можно сделать уже во время установки системы или в любое другое время. На практике чаще используется второй вариант, то есть настройка после установки: во время установки не всегда известны конкретные параметры сети организации, тем более внешним специалистам, которые обычно установку и выполняют.

Правильная конфигурация требует знания адресации протокола IP, устройства подсетей, других служб в сети, которые работают вместе с протоколом TCP/IP, например инструментов для устранения неполадок. Речь идет об очень большой теме, которая бы заняла целую книгу (и таких книг написано уже много). Это означает, что конфигурирование протокола TCP/IP для конкретной сети должен провести специалист, в котором вы уверены и знаете, что он ничего не забудет и все сделает правильно. Более подробные сведения о конфигурировании сети вы найдете дальше в этой главе.

Неоспоримым преимуществом протокола TCP/IP является его маршрутизируемость. На практике это означает, что с его помощью вы можете обратиться к любой удаленной сети (при условии, что с ней существует физическое соединение). Сеть, основанная на протоколе TCP/IP, может расти без ограничений. Достаточным доказательством этому утверждению служит существование сети Интернет.

Очень часто о TCP/IP говорят как о едином протоколе. На самом деле TCP/IP — это целый стек протоколов, состоящий из нескольких уровней. Для повседневной работы администратора необязательно знать эти подробности. В качестве примера протоколов, которые являются частью стека TCP/IP (с некоторыми из них вы уже встречались), можно назвать ICMP, IGMP, IP, TCP, HTTP, FTP, SMTP, SNMP, POP3, IMAP4 или NNTP. Протокол TCP/IP — это, безусловно, феномен сегодняшнего дня среди сетевых протоколов, и можно рекомендовать только лишь его. Даже при развертывании малой сети уместно с самого начала использовать TCP/IP, чтобы обеспечить возможность дальнейшего роста (на который должна рассчитывать каждая организация).

3.2.3. NWLink

Когда корпорация Novell выпустила свою операционную систему Novell NetWare, она готовила ее для коммуникации в сети при помощи собственного протокола IPX/SPX (Internetwork Packet Exchange/Sequenced Packet

Exchange). Она выпустила его только для своей системы, никогда не оглашала его подробности, и он навсегда остался только ее собственностью.

При появлении сетевых операционных систем Windows корпорация Microsoft сделала акцент на совместной работе своих сетевых клиентов с системой NetWare корпорации Novell. Изначально обе корпорации условились, что клиента для доступа к серверам NetWare, который станет частью Windows, будет создавать корпорация Novell. Позже перед корпорацией Microsoft встала проблема: как организовать коммуникацию собственных клиентов, работающих по протоколам NetBEUI или TCP/IP, с ресурсами NetWare с протоколом IPX/SPX? Следствием этого стала собственная реализация протокола IPX/SPX, которую в системах Windows 2000 и последующих корпорация Microsoft назвала NWLink.

Новые версии системы Novell NetWare уже содержат протокол TCP/IP. В этом случае отпадает необходимость устанавливать протокол NWLink, что значительно упрощает ситуацию и, как правило, делает ее прозрачнее.

Ответ на вопрос, какой протокол выбрать, таким образом, кажется однозначным. Если вы используете систему Windows и при этом хотите иметь надежную сеть, стабильный выход в Интернет и минимум временных и финансовых затрат на устранение неполадок, выбирайте только протокол TCP/IP. Ваша сеть будет быстрой, легко масштабируемой, основанной на стабильных и проверенных технологиях и готовой к подключению к Интернету. Каким способом протокол TCP/IP конфигурируется, какие инструменты нужны для настройки и как устранять неполадки, — об этом речь пойдет далее.

3.3. Адресация протокола TCP/IP

Даже если вы, установив протокол TCP/IP, оставите его в «первобытном» состоянии, есть вероятность, что ваши серверы и клиенты все-таки смогут общаться между собой. Однако рассчитывать на авось не стоит, тем более в сети масштаба предприятия: настраивать протокол TCP/IP все равно придется.

Для небольшой сети, объединяющей десяток-другой компьютеров, в настройке TCP/IP нет ничего сложного. Каждому компьютеру должен быть присвоен уникальный IP-адрес, маска подсети и в случае необходимости другие конфигурационные параметры, которые описаны далее.

IP-адреса

Чтобы компьютер мог общаться в сети по протоколу TCP/IP, ему должен быть присвоен IP-адрес, действительный в данной сети или подсе-

ти. IP-адрес — это 32-разрядное число, представленное в виде четырех восьмибитовых чисел (так называемые октеты), разделенных точками. Примеры IP-адресов:

- 1.2.3.4
- 102.13.16.237
- 216.254.1.18

Назначение IP-адреса должно подчиняться следующим основным правилам:

1. **Компьютеру нельзя присвоить первый адрес в данной сети** (адрес, заканчивающийся на число 0). Такие адреса зарезервированы для обозначения всей сети.
2. **Компьютеру нельзя присвоить последний адрес в данной сети** (адрес, заканчивающийся на число 255). Такие адреса служат для широковещательных передач (broadcasting) — обращения ко всем компьютерам в сети.
3. **Каждый из октетов — это число в диапазоне от 0 до 255**: восемью битами можно записать только 256 различных чисел.
4. **IP-адрес каждого компьютера должен быть уникален в пределах сети**. Если присвоить новому компьютеру уже существующий в сети адрес, то возникнет конфликт адресов. Операционная система сообщит о конфликте, показав окно предупреждения, и оба компьютера не будут допущены к работе в сети до исправления ситуации.

Как видно из этих правил, очень легко подсчитать, для скольких компьютеров найдется место в одной сети, работающей по протоколу TCP/IP. Теоретически IP-адреса могут быть любыми в диапазоне от 0.0.0.0 до 255.255.255.255, что составляет $2^{32} - 2 = 4\,294\,967\,294$.

На практике, однако, существуют еще некоторые ограничения, в результате которых предельное количество компьютеров в сети оказывается даже меньше. Так найдутся ли для вашей сети свободные адреса или нужно поверить скептикам, утверждающим, что диапазон IP-адресов уже почти исчерпан? Оказывается, верно и то, и другое: действительно диапазон адресов близок к исчерпанию, но для вашей сети адреса всегда найдутся.

Внутренние IP-адреса

О том, чтобы в распоряжении локальных сетей было достаточно IP-адресов, задумались задолго до того, как была установлена первая сеть под управлением ОС Windows 2000. Поскольку внутренние сети никак не связаны друг с другом, для адресации компьютеров в них можно использовать один и тот же диапазон IP-адресов.

Для локальных сетей, в зависимости от их размера, организацией IANA (Internet Assigned Numbers Authority), отвечающей за присвоение IP-адресов в Интернете, выделены следующие диапазоны адресов:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

Этих адресов вполне достаточно для организации сети, объединяющей несколько тысяч компьютеров. О любом адресе в такой сети можно с почти стопроцентной уверенностью утверждать, что он используется еще где-то. Однако беспокоиться о возможном конфликте адресов незачем: адреса из зарезервированных диапазонов действительны только в пределах локальной сети и ни с какой посторонней сетью не связаны.

Даже если вы собираетесь впоследствии подключить свою локальную сеть к Интернету, конфликта все равно не возникнет: об этом позаботятся технологии, известные как прокси-сервер или трансляция сетевых адресов (Network Address Translation, NAT). Эти технологии скрывают локальную сеть от внешнего мира, позволяя тем не менее сообщаться с Интернетом всем тем локальным компьютерам, которым это разрешил администратор.

Так как подавляющее большинство локальных сетей — малые, то есть объединяющие всего несколько десятков компьютеров, чаще всего для их адресации выбирают третий из зарезервированных диапазонов. Он предлагает 256 подсетей, каждая из которых может содержать не более 254 компьютеров (напоминаю, что первый и последний адреса из диапазона для адресации отдельного компьютера использовать нельзя) — итого 65024 компьютера.

Малую сеть можно логически разбить на подсети (например, относящиеся к разным подразделениям) произвольным образом. Для этого служит маска сети. Например, подсеть 192.168.10.0/24 объединяет компьютеры с адресами от 192.168.10.1 до 192.168.10.254.

Публичные IP-адреса

Очень упрощенно можно сказать, что публичными называются все те IP-адреса, которые не зарезервированы для локальных сетей. Это адреса, не относящиеся к сетям, рассмотренным в предыдущем пункте. Пример таких адресов — 111.112.113.114 или 170.180.190.200. Конечно, не каждый публичный адрес кем-то используется: многие компании, получив в свое распоряжение несколько IP-адресов, потом используют не все из них. Однако из того, что конкретный адрес не занят сейчас, отнюдь не следует, что завтра или через час он так и останется свободным.

Как видите, публичных адресов намного больше, чем внутренних. Разумеется, так и должно быть: всемирная сеть Интернет включает больше компьютеров, чем любая локальная сеть.

Примечание.

Когда вы подключаете свою локальную сеть к Интернету, свои публичные адреса вы уже не можете выбирать так же произвольно, как адреса локальных компьютеров. Вы должны получить их у своего провайдера, предоставляющего доступ в Интернет.

Внутренние IP-адреса и Интернет

Как уже было сказано выше, локальную сеть, использующую внутренние адреса, к Интернету подключить можно. Благодаря таким, например, технологиям, как трансляция сетевых адресов (NAT), адреса локальных компьютеров скрыты от внешнего мира. Более того, Интернет-маршрутизаторы не умеют работать с адресами, зарезервированными для внутреннего использования: если бы они получили пакет, направленный на такой адрес (например, ответ с веб-сервера корпорации Microsoft), то отбросили бы его без предупреждения, даже не попытавшись доставить по назначению.

Кто-нибудь бы мог сейчас задать простой вопрос: если адреса внутренней сети не видны извне, то не все ли равно, как их выбирать? Что мешает использовать в локальной сети адреса из публичных диапазонов? Ответ тоже прост. Если вы не собираетесь подключать локальную сеть к Интернету, то можете назначить внутренним компьютерам любые адреса.

Если же собираетесь, то обязательно выбирайте адреса из диапазонов, зарезервированных для локальных сетей. В противном случае, хоть ваша сеть и будет работать надежно, вы не получите доступа к Интернет-серверам, адреса которых совпадают с теми, которые вы выбрали для локальных компьютеров. А что если это окажутся очень важные серверы?

Маска подсети

Маска подсети — это 32-разрядное число, которое подобно IP-адресу делится на 4 октета по 8 битов. Ее роль в IP-адресации очень велика, так как именно маска определяет, находятся ли компьютеры в одной подсети так, что они могут общаться напрямую, или же их коммуникация должна проходить через маршрутизатор.

Приведем простой пример. Для сетей класса C (к этому классу относятся локальные сети, в первом октете адреса которых стоит число 192) маска

подсети по умолчанию равна 255.255.255.0. Записав ее в двоичной системе, получим 11111111.11111111.11111111.00000000. Теперь запишем IP-адрес и маску друг под другом:

11000000.10101000.00001010.00000001 — IP-адрес (192.168.10.1)

11111111.11111111.11111111.00000000 — маска подсети (255.255.255.0)

Та часть IP-адреса, которой соответствуют единицы маски, распознается как адрес подсети, а те двоичные разряды, которым соответствуют нули маски, — как адрес узла (компьютера) внутри подсети. Узлы одной подсети (192.168.10.2, 192.168.10.3 и т.д.) «видят» друг друга непосредственно, а для коммуникации между узлами разных подсетей (например, 192.168.10.1 и 192.168.11.1) необходим маршрутизатор.

В пункте 3.3.2 мы выбрали для сети адрес 192.168.10.0/24. Что означает эта запись?

Маска подсети — это такое число, в двоичной записи которого все единицы предшествуют всем нулям, что естественно: в IP-адресе разряды, отведенные под адрес подсети, предшествуют разрядам, отведенным под адрес узла. Такие числа однозначно определяются количеством единиц в них. Подсчитайте единицы в числе 11111111.11111111.11111111.00000000 — их 24. Выражение /24 — это запись той же самой маски подсети 255.255.255.0 в нотации CIDR (Classless InterDomain Routing).

Примечание.

Последний октет маски подсети не обязан быть нулевым. Можно логически разбить одну сеть на несколько, «позаимствовав» несколько разрядов, обычно отводимых под адрес узла, и использовав их для адресации подсетей. Так, маска 255.255.255.192, последний октет которой в двоичной записи выглядит как 11000000, позволяет создать четыре сети с 62 (64-2, напоминаю, что первый и последний адреса в подсети зарезервированы для специальных целей) узлами в каждой.

В более крупных сетях вы можете встретить маску 255.255.0.0 и даже 255.0.0.0. Рассмотрение этих случаев выходит за рамки нашей книги.

3.4. Установка протокола TCP/IP

Протокол TCP/IP в операционных системах Windows 2000 и последующих устанавливается автоматически в ходе установки системы. При типичной установке TCP/IP является единственным установленным протоколом (рис. 3.2).

Сам протокол лишь обеспечивает возможность коммуникации между компьютерами. Для нормальной работы пользователя в системе должны быть установлены еще и другие службы и клиенты.

Клиент сети Microsoft

Клиент сети Microsoft — это сетевой компонент, позволяющий компьютеру использовать возможности, предоставляемые сетью под управлением операционных систем Microsoft. Если этот компонент не установлен, то пользователь клиентского компьютера не может подключиться к общим папкам, печатать на сетевых принтерах и т.п. Такая связь с точки зрения пользователя совершенно бесполезна.

Как говорит название, этот компонент предназначен только для работы в сети Microsoft. Если вы хотите использовать сетевые возможности операционной системы Novell NetWare, то необходимо кроме протокола NWLink устанавливать и клиента системы NetWare.

Клиента сети Microsoft не нужно конфигурировать. Единственным конфигурационным пунктом, который появляется после нажатия кнопки **Свойства**, является **Служба удаленного вызова процедур** (Remote Procedure Call). По умолчанию в Windows XP Professional эту функцию выполняет **Локатор системы** Windows, что соответствует нашим задачам.

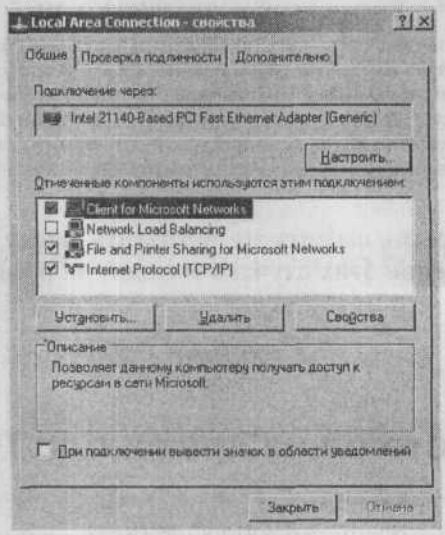


Рис. 3.2. *Диалоговое окно свойств подключения к локальной сети в Windows XP Professional*

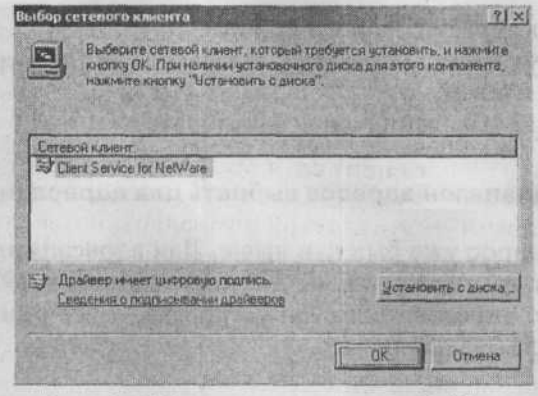


Рис. 3.3. *Установка клиента сети NetWare*

Служба доступа к файлам и принтерам сетей Microsoft

Эта сетевая служба в некотором смысле противоположна Клиенту для сетей Microsoft. Ее назначение в том, чтобы разделяемые папки и принтеры того компьютера, на котором работает эта служба, были в распоряжении удаленных пользователей (других компьютеров в сети). Полностью ситуацию можно описать так: Клиент сети Microsoft на локальном компьютере общается со Службой доступа к файлам и принтерам сетей Microsoft на удаленном компьютере и наоборот.

Служба доступа к файлам и принтерам сетей Microsoft в операционной системе Windows XP Professional *настройке не подлежит.*

Для полноценной работы в сети компьютера с Windows XP Professional необходимы все три вышеназванных компонента: протокол сети Интернет (TCP/IP), Клиент для сетей Microsoft, Служба доступа к файлам и принтерам сетей Microsoft.

3.5. Настройка протокола TCP/IP

3.5.1. Подготовка к настройке

К настройке протокола TCP/IP следует тщательно подготовиться. Необходимо решить следующие вопросы:

- Какой диапазон адресов выбрать для адресации сети?
- Какие IP-адреса назначить серверам?
- Какие IP-адреса назначить принтерам и подобным им устройствам?
- Какие IP-адреса назначить клиентским компьютерам?

- Каким будет адрес основного шлюза?
- Какими будут другие параметры протокола IP (серверы DNS, WINS, имя домена и т.п.)?
- Какой способ выделения адресов выбрать?

Какой диапазон адресов выбрать для адресации сети

Ответ на этот вопрос уже был дан выше. Для адресации сети с несколькими десятками компьютеров мы выбрали диапазон 192.168.10.0/24. В этой сети можно адресовать до 254 устройств, и все они должны иметь маску подсети 255.255.255.0.

Примечание.

Если вы предполагаете, что скоро (скажем, в течение года) количество устройств в сети значительно увеличится, то разумно будет с самого начала выбрать более широкий диапазон адресов, который позволял бы подключить больше 254 устройств.

Какие IP-адреса назначить серверам

Определенный диапазон адресов нужно зарезервировать для использования исключительно серверами. Длина этого диапазона зависит от количества серверов — имеющихся сейчас и предполагаемых в дальнейшем. В нашей сети пока есть единственный сервер, и даже с учетом будущего роста сети их не будет больше десяти. Для серверов мы выделим IP-адреса с 192.168.10.2 до 192.168.10.11.

Какие IP-адреса назначить принтерам и подобным им устройствам

В сети нашего размера разумно выделить для принтеров и другого сетевого оборудования пять адресов. Мы зарезервируем за ними адреса от 192.168.10.12 до 192.168.10.16.

Какие IP-адреса назначить клиентским компьютерам?

Все оставшиеся адреса — от 192.168.10.17 по 192.168.10.254 — будут розданы клиентским компьютерам. Таким образом, в нашей сети не может быть больше 238 компьютеров.

Каким будет адрес основного шлюза

Основной шлюз, или маршрутизатор — это устройство, соединяющее локальную сеть (подсеть) со внешним миром. На это устройство все узлы

данной подсети отправляют пакеты, предназначенные для узла в другой подсети или в Интернете.

Поскольку наша сеть пока будет сама по себе, то есть не мы не подключаем ее ни к Интернету, ни к другой локальной сети, в основном шлюзе нет необходимости. Однако на будущее нужно зарезервировать за ним IP-адрес. Обычной практикой является назначение шлюзу первого адреса в данной сети — в нашем случае это адрес 192.168.10.1.

Какими будут другие параметры протокола IP

В этом месте следует собрать воедино другие конфигурационные параметры протокола IP. К ним относятся IP-адреса сервера (или серверов) DNS, сервера (или серверов) WINS, тип узла компьютера, имя домена и т.д. В следующих главах мы рассмотрим каждый из этих параметров подробнее.

Какой способ выделения адресов выбрать

Наш диапазон IP-адресов дает возможность адресовать до 254 сетевых устройств. Адрес 192.168.10.0 означает всю сеть, и его нельзя использовать для адресации отдельных устройств. Адрес 192.168.10.255 служит для передачи широковещательных (broadcast) сообщений, то есть сообщений, предназначенных для каждого устройства в сети. Это стандартная установка протокола TCP/IP в системе Windows, которую нет необходимости конфигурировать дальше. После того, как мы выделили IP-адреса для серверов, принтеров и других устройств, у нас в распоряжении осталось 238 адресов для клиентских компьютеров. Теперь нужно решить, будем ли мы назначать адреса клиентским компьютерам вручную или автоматически по протоколу DHCP. Оба способа имеют как свои преимущества, так и недостатки, а иногда автоматическое выделение адресов вообще невозможно. В этой главе описана настройка протокола TCP/IP вручную, но это не значит, что такое решение оптимально. Оно всего лишь проще и пригоднее для объяснения основ настройки сети. Сведения об автоматическом выделении адресов вы найдете в 8 главе.

Влиять на выбор IP-адресов могут и другие факторы. Необходимо хорошо продумать все особенности вашей сетевой среды и тщательно подготовиться к настройке протокола TCP/IP. В дальнейшем смена адресации может быть для пользователей и администраторов весьма долгим и трудным процессом.

3.5.2. Настройка протокола TCP/IP на сервере

Сервер присутствует в сети для того, чтобы предоставлять услуги другим компьютерам. Это может быть файловый сервер (то есть сервер, на котором в разделяемых папках хранятся документы предприятия), сервер приложений (например, если на нем установлена база данных), веб-сервер (сервер, на котором установлены веб-службы: WWW, FTP, новостной протокол NNTP и т.п.), почтовый сервер (сервер, предназначенный для приема или передачи электронной почты и управления почтовыми ящиками) или, например, сервер печати, то есть компьютер, который обрабатывает задания на печать и отсылает их локальным принтерам. Кроме перечисленных услуг пользователям, сервер может обслуживать и саму сетевую инфраструктуру (службы DHPS, DNS, WINS или сертификации документов).

Чтобы компьютеры-клиенты могли обращаться к серверу с запросом услуг, они должны знать его IP-адрес или имя, которое где-то в пределах сети связано с IP-адресом таким же образом, как в телефонном справочнике название предприятия связано с его телефонным номером. Этот IP-адрес должен быть постоянным, потому что его изменение могло бы нарушить связь между компьютерами пользователей и сервером. А если сервер сам предоставляет услуги DHCP или DNS, то такому серверу постоянный адрес тем более необходим.

Назначать серверам IP-адреса и другие конфигурационные параметры всегда следует вручную. Тогда вы будете уверены, что IP-адрес ни в коем случае не изменится, и сможете быстро найти адрес по серверу и сервер по адресу. Это необходимо для устранения неполадок в сети. Одним словом, хороший администратор должен знать адреса своих серверов наизусть.

Чтобы настроить параметры протокола TCP/IP на сервере, выполните следующие действия:

1. В меню **Пуск** выберите **Панель управления → Сетевые подключения → Подключение по локальной сети**.
2. В появившемся диалоговом окне состояния на вкладке **Общие** нажмите кнопку **Свойства**. Отобразится диалоговое окно **Подключение по локальной сети — свойства**.
3. В списке компонентов, используемых этим подключением, выберите пункт **Протокол Интернета (TCP/IP)** и нажмите кнопку **Свойства**.
4. В диалоговом окне **Свойства: протокол Интернета (TCP/IP)** (рис.3.4) установите переключатель в положение **Использовать следующий IP-адрес** и в поле **IP-адрес** введите значение 192.168.10.2.
5. В поле **Маска подсети** введите значение 255.255.255.0.

Рис. 3.4. *Диалог настройки протокола TCP/IP на сервере*

6. В нижней части окна свойств установите переключатель в положение **Использовать следующие адреса серверов DNS** и в поле **Предпочитаемый DNS-сервер** введите значение 192.168.10.2 (наш сервер будет служить сервером DNS сам себе). Затем нажмите кнопку **Дополнительно**. Более подробно о настройке службы DNS будет сказано в 6 главе.

Примечание.

Если вы неправильно укажете адрес сервера DNS, то не будет работать домен и у пользователей могут возникнуть проблемы с регистрацией.

7. На вкладке **DNS** убедитесь в том, что установлены переключатель **Дописывать основной DNS-суффикс и суффикс подключения** и флажки **Дописывать родительские суффиксы осн. DNS-суффикса** и **Зарегистрировать адреса этого подключения в DNS**. Нажмите **OK**.
8. Нажатием на кнопку **OK** закройте диалоговое окно свойств протокола TCP/IP.
9. Включите флажок **При подключении вывести значок в области уведомлений** и нажмите кнопку **Закрыть**.
10. Нажатием на кнопку **Закрыть** закройте диалоговое окно состояния подключения по локальной сети. В углу панели задач появится значок только что настроенного вами подключения.

Примечание.

Если вы включите переключатель **Использовать следующие адреса серверов DNS**, но не укажете ни одного адреса, то в ОС Windows 2000 Server будет автоматически введен адрес 127.0.0.1. Это адрес локального интерфейса (loopback), через который общаются между собой процессы, работающие на одном компьютере. Если сервер является в то же время сервером DNS, то клиент DNS будет нормально работать, обращаясь по этому адресу. Любопытно, что адрес 127.0.0.1 нельзя ввести вручную.

3.5.3. Настройка протокола TCP/IP на компьютере-клиенте

Клиентские компьютеры подключаются к сети для того, чтобы пользоваться услугами различных сетевых служб. Чтобы они могли взаимодействовать по протоколу TCP/IP, этот протокол нужно правильно настроить. Вообще говоря, не слишком важно, чтобы два клиента могли общаться непосредственно (в самом деле, какими данными им обмениваться — разве что файлами MP3?) Намного важнее возможность коммуникации между клиентом и сервером. Клиенту нужно взаимодействовать также с контроллером домена, который обеспечивает регистрацию пользователя; с сервером DNS, который сопоставляет запрошенным именам IP-адреса; с файловым сервером, на котором хранятся документы предприятия; с сервером печати, на который отсылаются задания, и так далее. При правильно настроенном протоколе TCP/IP любой компьютер в сети может общаться с любым другим, если администратор не вводил никаких ограничений.

Клиентскому компьютеру совсем не обязательно иметь постоянный IP-адрес, поэтому его можно настраивать не только вручную, но и автоматически. Подробнее об автоматическом выделении адреса мы поговорим в следующих главах, потому что оно требует еще некоторых настроек на сервере. Сейчас же мы посмотрим, как производится ручная настройка.

Чтобы настроить параметры протокола TCP/IP на сервере, выполните следующие действия:

1. В меню **Пуск** выберите **Панель управления → Сетевые подключения → Подключение по локальной сети**.
2. В появившемся диалоговом окне состояния на вкладке **Общие** нажмите кнопку **Свойства**. Отобразится диалоговое окно **Подключение по локальной сети — свойства**.
3. В списке компонентов, используемых этим подключением, выберите пункт **Протокол Интернета (TCP/IP)** и нажмите кнопку **Свойства**.
4. В диалоговом окне **Свойства: протокол Интернета (TCP/IP)** (рис. 3.5) установите переключатель в положение **Использовать следую-**

щий IP-адрес и в поле **IP-адрес** введите адрес из диапазона, отведенного нами для клиентских компьютеров — 192.168.10.17.

5. В поле **Маска подсети** введите значение 255.255.255.0.
6. В нижней части окна свойств установите переключатель в положение **Использовать следующие адреса серверов DNS** и в поле **Предпочитаемый DNS-сервер** введите значение 192.168.10.2 (для всех клиентов сервером DNS будет служить сервер, настройка которого рассматривалась в предыдущем пункте). Нажмите кнопку **Дополнительно**.

Примечание.

Если вы неправильно укажете адрес сервера DNS, то не будет работать домен и у пользователей могут возникнуть проблемы с регистрацией.

7. На вкладке **DNS** убедитесь в том, что установлены переключатель **Дописывать основной DNS-суффикс и суффикс подключения** и флажки **Дописывать родительские суффиксы осн. DNS-суффикса** и **Зарегистрировать адреса этого подключения в DNS**. Нажмите **OK**.
8. Нажатием на кнопку **OK** закройте диалоговое окно свойств протокола TCP/IP.
9. Включите флажок **При подключении вывести значок в области уведомлений** и нажмите кнопку **Закрыть**.
10. Нажатием на кнопку **Закрыть** закройте диалоговое окно состояния подключения по локальной сети. В углу панели задач появится значок только что настроенного вами подключения.

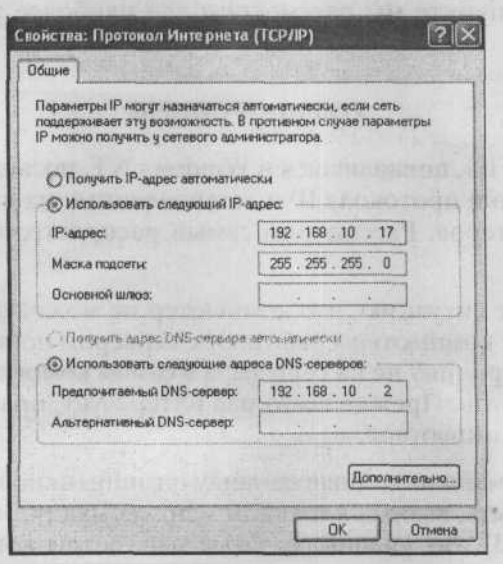


Рис. 3.5. *Диалог настройки протокола TCP/IP на клиенте*

Последующие клиентские компьютеры настраивайте точно так же, только на шаге 4 задавайте адрес из клиентского диапазона, отличный от уже введенных: 192.168.10.18, 192.168.10.19 и т.д.

3.6. Проверка связи

После установки и настройки протокола TCP/IP обязательно нужно проверить, успешно ли компьютер подключился к сети. При этом вы сможете выявить и устранить неполадки до того, как они проявятся в ходе повседневной работы. Отсутствие или ошибки связи по протоколу TCP/IP могут быть обусловлены множеством причин. Чаще всего это неправильная установка протокола, физическое прерывание связи между компьютерами в сети, неправильное задание IP-адреса или отсутствие совместимости между протоколом и сетевым адаптером.

Далее мы рассмотрим, как можно выявить и устранить эти неисправности.

3.6.1. Инструменты для проверки связи по протоколу TCP/IP

Операционные системы Windows, начиная с Windows 2000, содержат целый ряд утилит, служащих для настройки и отладки связи по протоколу TCP/IP. В этом пункте мы рассмотрим две наиболее употребительные из них.

Утилита IPCONFIG

Утилита IPCONFIG, появившаяся в Windows NT, позволяет просмотреть текущие настройки протокола IP и установленных на данном компьютере сетевых адаптеров. Рассмотрим самый распространенный способ ее применения.

Представьте себе ситуацию, что компьютер не может связаться с сервером. Если другие компьютеры работают с сервером нормально, то вполне логично искать причину не на сервере, а в самом компьютере, который не поддерживает связь. Прежде всего нас интересует, правильно ли указан IP-адрес этого компьютера.

- Введите в командной строке команду **ipconfig** (окно командной строки можно открыть, выбрав в главном меню команду **Выполнить** и введя команду cmd). Вы увидите базовые параметры конфигурации узла: IP-адрес, маску подсети и адрес основного шлюза.

- Если вы введете команду **ipconfig** с ключом **/all**, то будет выведена полная информация о настройках протокола TCP/IP.

Вы должны увидеть тот IP-адрес, который указывали при настройке клиентского компьютера (от 192.168.10.17 до 192.168.10.254), и маску подсети 255.255.255.0. Если отобразятся другие значения, исправьте настройки так, как указано в п.3.5.3. Маска 0.0.0.0 говорит о том, что указанный вами IP-адрес уже используется другим узлом в этой же сети — возник конфликт адресов.

Примечание.

Посредством утилиты IPCONFIG можно только просматривать информацию об IP-адресе, маске подсети и других параметрах, но не изменять ее.

Утилита PING

Для проверки соединения между двумя узлами служит утилита PING, тоже давно входящая в состав ОС Windows. Эта утилита посылает на указанный узел пакеты эхо-запроса протокола ICMP и считает полученные от него пакеты эхо-ответа, чтобы проверить, доступен ли этот узел вообще и надежна ли связь (какова доля пакетов, потерявшихся по дороге). Последовательно тестируя соединения с каждым узлом, можно обнаружить место, в котором связь оборвалась.

При получении эхо-ответа утилита PING выводит следующее сообщение:

```
Ответ от 192.168.10.17: число байт=32 время [...]
```

Время в миллисекундах — это промежуток времени между посылкой запроса и получением ответа. Чем больше это время, тем «дальше» расположенным можно считать узел.

Команда **ping** может дать и отрицательный ответ:

- **Превышен интервал ожидания для запроса**: эхо-ответ от узла не получен в течение заданного времени ожидания. Причиной может быть неправильная работа компьютера, от которого ожидается ответ (возможно, он просто выключен или отключен от сети). Может случиться также, что где-то на пути связи между двумя компьютерами заблокирован протокол ICMP.
- **Заданный узел недоступен**: невозможно отправить эхо-запрос на указанный узел: путь к нему неизвестен. Причина этого — ошибка маршрутизации. Скорее всего вы не указали IP-адрес основного шлюза, через который пакеты из локальной сети уходят во внешний мир, но может быть и ошибка в таблице маршрутизации на тестируемом компьютере или на самом шлюзе. Просмотреть таблицу маршрути-

зации можно по команде **route print.** Команда **route** без аргументов выводит краткую справку об использовании утилиты ROUTE.

По умолчанию команда **ping** делает 4 попытки послать пакет размером 32 байта. Оба значения можно изменить при помощи соответствующих ключей: команда **ping** без аргументов выводит краткую справку о допустимых ключах и их назначении.

Последовательность диагностики сети должна быть такой:

1. В командной строке введите команду **ping 127.0.0.1**. Эта команда проверит работоспособность локального интерфейса (см. примечание к п.3.5.2). Локальный интерфейс не имеет никакого отношения к физическим сетевым адаптерам: это «виртуальный адаптер», служащий только для проверки стека протоколов TCP/IP. Если вы получите ответ от локального интерфейса, значит, по крайней мере в локальной системе все в порядке. Если вы ответа не получите (Статистика Ping сообщает «100% потерь»), то проблема однозначно в неправильной установке протокола TCP/IP. Но поскольку этот протокол устанавливается вместе с операционной системой, то можно сказать, что проблема в неправильной установке операционной системы.
2. В командной строке введите команду **ping 192.168.10.17** (IP-адрес того компьютера, который вы сейчас проверяете). Это следующий шаг «самопроверки»: после того, как вы выяснили, что с установкой протокола TCP/IP все в порядке, нужно прозондировать собствен-

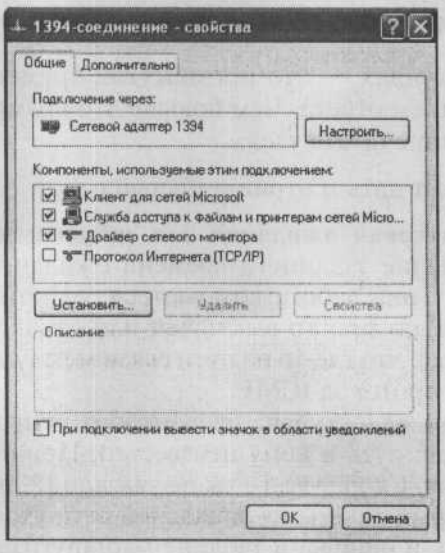


Рис. 3.6. *Протокол TCP/IP не привязан к сетевому адаптеру*

ный сетевой адаптер. Если не отвечает эта команда, то проблема в нем. Причин ошибки может быть две.
Первая — сам адаптер: неаккуратно вставлен, неисправен или не установлены нужные драйвера. Эта причина встречается чаще всего.
Вторая причина — протокол TCP/IP не привязан к данному сетевому адаптеру (рис.3.6). Обычно это происходит, когда на вашем компьютере установлено несколько сетевых карт и вы забыли настроить TCP/IP на некоторых из них.

3. Теперь проверьте связь с соседним компьютером, заведомо подключенным к сети, или сервером: **ping 192.168.10.2**. Если ответа нет, в то время как все остальные компьютеры сети соединяются с сервером нормально, то причина — физический разрыв соединения между тестируемым компьютером и сетью (ближайшим хабом): сетевой кабель неисправен или выпал из разъема; может быть также неисправен порт хаба.

Если проверка показала, что ваш компьютер успешно подключен к сети, вы можете проверить, работает ли служба разрешения имен узлов в IP-адреса. Выполните команду **ping** с именем компьютера вместо IP-адреса: **ping SRVR001**. Если вы не получите ответа, значит, неправильно работает служба DNS, сопоставляющая имена компьютеров IP-адресам. Эта служба будет подробнее рассмотрена в дальнейших главах, а пока достаточно того, что работает сама сеть.

3.6.2. Сетевой адаптер и несколько протоколов

Если на компьютере установлено несколько протоколов (неважно, по какой причине — исторически ли так сложилось, администратор ли экспериментировал), или, иными словами, если компьютер умеет говорить на нескольких языках, то это создает избыточную нагрузку на сеть.

Для оптимальной загрузки сети и надежной работы сетевых служб рекомендуется использовать только самые необходимые протоколы. В абсолютном большинстве случаев достаточно одного протокола TCP/IP.

Рассмотрим, как происходит коммуникация двух компьютеров, на одном из которых установлены два протокола — TCP/IP и NWLink. В нашей сети мы еще не устанавливали протокол NWLink, но для примера будем считать, что это уже сделано.

Когда в ОС Windows 2000 и выше устанавливается новый протокол, то он автоматически привязывается ко всем имеющимся на компьютере сетевым адаптерам. На каждом адаптере эти привязки образуют иерархию, или порядок. Порядок привязки определяет очередность выполнения протоколов: если с одной сетевой картой связано несколько протоколов, то при попытке установить соединение с удаленным узлом операционная

система сначала обратится к нему по первому протоколу, если соединение не удастся — по следующему, и так далее.

Просмотреть порядок привязки можно следующим способом:

1. В меню **Пуск** выберите **Панель управления.** Щелкните правой кнопкой мыши по пункту **Сетевые подключения** и в контекстном меню выберите команду **Открыть.**
2. В окне папки **Сетевые подключения** выберите из меню команду **Дополнительно → Дополнительные параметры** и в появившемся окне открыть вкладку **Адаптеры и привязки** (рис. 3.7).

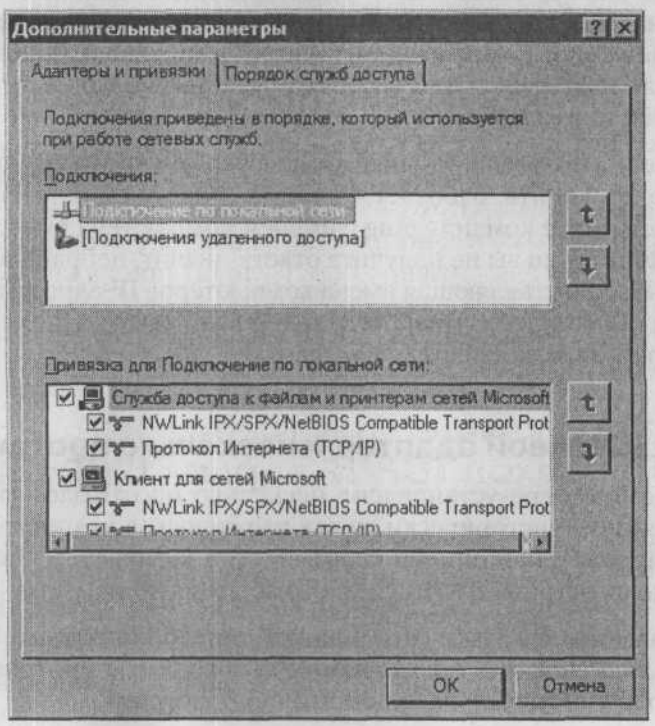


Рис. 3.7. *Привязки протоколов к сетевым адаптерам*

На рисунке видно, что первым в иерархии привязок стоит протокол NWLink. Если на соседнем компьютере, с которым мы пытаемся установить соединение, тоже установлен NWLink, то первая попытка связи окажется успешной и эти два узла будут общаться друг с другом по протоколу NWLink, а со всеми остальными узлами сети — по TCP/IP. Если же на втором компьютере стоит только TCP/IP, то одна и та же информация будет послана дважды: сначала по протоколу NWLink — неудачно, потом по TCP/IP — успешно. Вот так сеть и засоряется ненужной информацией.

Что же делать, если условия требуют поддерживать протокол NWLink — например, ради одного-единственного узла, понимающего только этот протокол? Можно изменить порядок привязки: поставить TCP/IP первым. Тогда лишние пакеты будут отправляться в сеть только при попытках соединиться с этим единственным узлом.

Чтобы изменить очередность выполнения протокола, в диалоговом окне **Дополнительные параметры** (рис. 3.7) выберите нужный протокол и нажатием на кнопку со стрелкой в правой части диалогового окна передвиньте его вверх или вниз.

Если вы полагаете, что ваша сеть еще слишком мала для того, чтобы учитывать такие тонкости, взвесьте ситуацию еще раз. Если вы присмотритесь к работе сети, то заметите, что в каждый момент времени информацию может передавать только один узел. Если несколько узлов попытаются связаться друг с другом одновременно, то в сети Ethernet возникнет конфликт, будет разрешен в пользу одного из них, а остальным придется повторить попытку через некоторое время. При избыточной установке нескольких протоколов даже в малой сети может происходить изрядное количество сбоев, потому что по ней путешествует в несколько раз больше пакетов, чем нужно и чем было бы при наличии единственного протокола.

3.7. Будущее протокола TCP/IP. Протокол TCP/IP версия 6 (IPv6)

Всемирная сеть Интернет постоянно растет, и уже довольно давно высказываются опасения, что свободные IP-адреса скоро кончатся. Наступает время, когда этой проблемой придется заняться вплотную. Одно из последних предложенных решений — новая версия протокола IP — IPv6.

Протокол IP был разработан в 1981 году и с тех пор ни разу не менялся. Но среда, в которой он работает, изменилась до неузнаваемости. Разработчики протокола IP не рассчитывали на следующие требования, предъявляемые современными сетями:

- **В связи с экспоненциальным ростом количества узлов нужен значительно больший диапазон возможных IP-адресов.** Сейчас узлы локальных сетей выходят в Интернет через очень небольшое количество шлюзов с публичными адресами, используя методы вроде NAT. А в более крупных локальных сетях скоро перестанет хватать адресов из внутреннего диапазона.
- **Маршрутизаторам, обеспечивающим доступность любого узла в сети, необходимо уметь работать с большими таблицами маршрутизации.**

Главным маршрутизаторам Интернета сейчас приходится обрабатывать таблицы, содержащие более 85000 записей.

- **Простота настройки.** Хотя сейчас протокол IP можно настраивать как вручную, так и автоматически при помощи протокола DHCP, велика потребность в дальнейшем упрощении этой процедуры.
- **Обеспечение безопасности на уровне протокола IP.** Передача конфиденциальных данных требует гарантии их защиты. Для этой цели уже разработан стандарт — протокол IPSec — однако он абсолютно не обязателен для работы сети и устанавливается по желанию.

Усовершенствованный протокол IPv6 отвечает этим требованиям. Среди самых важных особенностей следует отметить длину адреса (она составляет 128 битов — в 4 раза больше, чем у нынешнего протокола IPv4, что многократно увеличивает диапазон возможных адресов), автоматическую настройку IP-адреса при помощи сервера DHCP или без него, встроенный протокол IPSec и гибкую масштабируемую структуру маршрутизации.

Протокол IPv6 несовместим с IPv4. Чтобы подключить к Интернету сеть, работающую по протоколу IPv6, нужно использовать механизм, преобразующий пакеты IPv6 в пакеты протокола IPv4, то есть шлюз такой сети обязан поддерживать оба протокола.

Протокол IPv6 входит в состав Windows XP и ОС семейства Windows 2003. Способы его установки в различных системах различны. Если в Windows Server 2003 его можно установить так же, как любой другой протокол (рис. 3.8), то в ОС Windows XP для установки IPv6 необходимо ввести **ipv6 install** в командной строке.

Описание протокола IPv6 — тема, которой бы хватило на отдельную книгу, поэтому рассмотрение его подробностей выходит далеко за пределы этой главы. Вам не нужно устанавливать IPv6 прямо сейчас, потому что

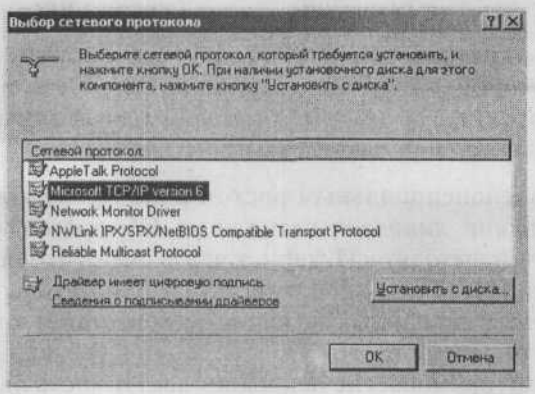


Рис. 3.8. *Установка протокола IPv6 в системе Windows Server 2003*

мы пока не собираемся с ним работать. Когда-нибудь этот протокол может вам пригодиться, а пока достаточно знать, что ОС семейств Windows XP и Windows Server 2003 его поддерживают.

3.8. Итоги

В этой главе вы выбрали протокол для своей локальной сети и настроили протокол TCP/IP на сервере и рабочих станциях. Сначала вы выбрали диапазон IP-адресов (подсеть) 192.168.10.0/24, потом подготовились к назначению адресов всем сетевым устройствам и, наконец, произвели саму настройку. Настройка протокола TCP/IP во всех примерах проведена вручную. Далее вы проверили работу сети с помощью утилиты PING.

Вы узнали об инструментах, позволяющих выявить и устранить неполадки в работе сети.

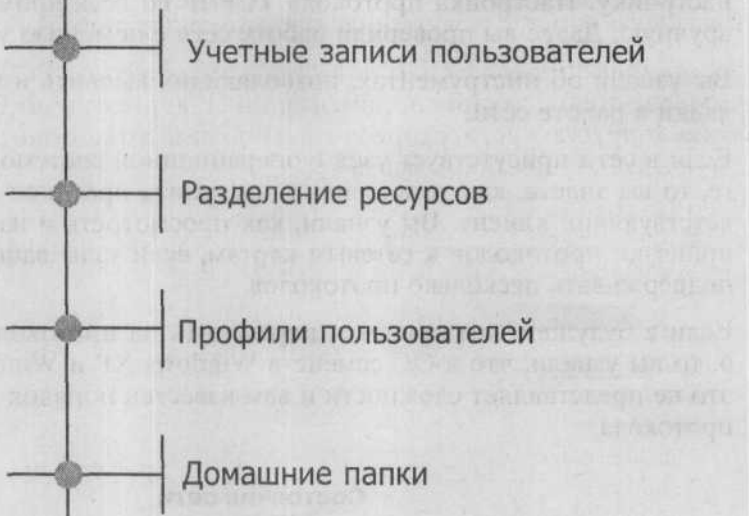
Если в сети присутствует узел с операционной системой Novell NetWare, то вы знаете, как установить и настроить протокол NWLink и соответствующий клиент. Вы узнали, как просмотреть и изменить порядок привязки протоколов к сетевым картам, если узлы вашей сети должны поддерживать несколько протоколов.

Если в будущем вам придется переходить на протокол TCP/IP версии 6, то вы узнали, что в ОС семейств Windows XP и Windows Server 2003 это не представляет сложности и вам известен порядок установки этого протокола.

Состояние сети

Состояние сети в этой главе не изменилось.

Глава 4 Организация рабочей группы



После успешной установки мы имеем в распоряжении один сервер и несколько рабочих станций. В ходе чтения этой книги мы разворачиваем малую сеть, которая до конца книги еще претерпит изрядное количество изменений. Целью этих изменений будет, с одной стороны, приспособление к конкретным потребностям и возможностям предприятия, а с другой стороны — удовлетворение потребностей пользователей.

В этой главе речь пойдет о том, как обеспечить работу пользователей в сети, то есть о том, чтобы на рабочих станциях мог бы работать еще кто-то кроме администратора.

4.1. Учетные записи пользователей

Чтобы пользователь вообще мог начать работу за рабочей станцией, ему должна быть разрешена регистрация на ней. Кроме того, нужно, чтобы каждому пользователю была обеспечена хотя бы небольшая степень свободы, то есть чтобы каждый из них мог отрегулировать свое рабочее пространство в соответствии с собственными потребностями, не нарушая при этом общих принципов предприятия.

Важно также, чтобы он обладал исключительным правом доступа к своим документам. Исходя из этого, не следует разрешать всем пользователям регистрироваться под одной и той же учетной записью и тем более не стоит предоставлять им права пользователя «Администратор». То есть для каждого пользователя нужно создать собственную учетную запись.

4.1.1. Создание учетной записи

Учетные записи пользователей, созданные на рабочей станции, хранятся в локальной базе данных SAM (Security Accounts Manager). Они позволяют зарегистрироваться только на том компьютере, на котором находится эта база. Если пользователю нужно работать за другим компьютером, необходимо создать для него учетную запись и там. Значит, если четырем вашим пользователям требуется возможность работать за любым из четырех компьютеров, то всего придется создать 16 учетных записей — по 4 на каждом компьютере.

1. Зарегистрируйтесь на одной из рабочих станций под именем Администратор.
2. Выберите в главном меню **Панель управления → Администрирование → Управление компьютером**. Если вы переключили главное меню на классический вид, то папку **Панель управления** вы найдете в группе **Настройка**, а элемент **Администрирование** — под иконкой **Производительность и обслуживание**.
3. В окне консоли **Управление компьютером**, в левой части, раскройте объект **Локальные пользователи и группы**, а затем щелкните правой кнопкой мыши по появившейся в правой части окна иконке **Пользователи.** В контекстном меню выберите пункт **Новый пользователь.**
4. В поле **Пользователь** (рис. 4.1) введите регистрационное имя (то имя, которое пользователь будет вводить при входе в систему).

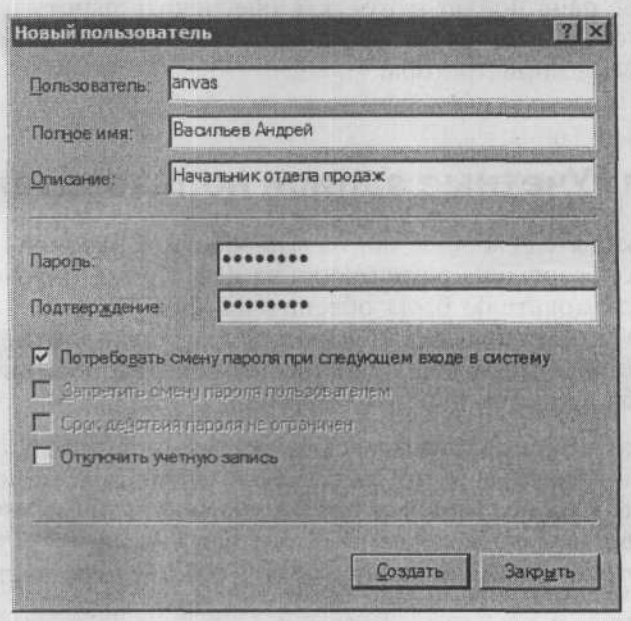


Рис. 4.1. *Диалоговое окно* ***Новый пользователь***

Примечание редактора.

В регистрационных именах лучше обойтись без букв кириллицы, поскольку многие программы при установке требуют сведений о пользователе, а далеко не все производители ПО включают поддержку кириллицы. Например, программа Mathlab 7 просто отказывается работать на таком компьютере, у которого имена пользователей записаны кириллицей.

5. В поле **Полное имя** введите фамилию и имя пользователя. В поле **Описание** вы можете как-то охарактеризовать этого пользователя (например, указать должность). Эти поля необязательны, информация в них нужна только для справки, и ее можно вводить кириллицей.

Совет.

Имеет смысл фамилию указывать перед именем: тогда у вас будет возможность сортировать учетные записи по фамилиям.

6. В поля **Пароль** и **Подтверждение пароля** введите пароль, с которым пользователь сможет зарегистрироваться на этом компьютере. После того, как вы сообщите пароль новому пользователю, этот пароль будут знать два человека: он сам и администратор, то есть вы. Чтобы избавить пользователей от этого неудобства, установите флажок **Потребовать смену пароля при следующем входе в систему**: теперь пользователь сможет указать пароль, который будет знать только он сам. Более того, он должен это сделать: пока он не сменит пароль, ему не будет разрешено начать сеанс работы.

Примечание.

Обязательно объясните своим коллегам, что для обеспечения достойной степени конфиденциальности пароль должен быть «сильным», т.е. состоять из разумного количества заглавных и строчных букв, цифр и специальных знаков. Покажите наглядно, как составлять такой пароль, на примере первичного пароля, который создадите сами и сообщите новому пользователю.

7. Нажмите кнопку **Создать** и закройте окно **Новый пользователь** нажатием на кнопку **Закрыть**.

4.1.2. Настройка учетной записи

Создание учетной записи — только первый шаг. Теперь нужно указать ее дальнейшие свойства. Эта процедура называется настройкой.

1. В окне консоли **Управление компьютером** откройте папку **Пользователи** и щелкните по новой записи правой кнопкой мыши. В контекстном меню выберите команду **Свойства**.

2. На вкладке **Членство в группах** убедитесь, что новый пользователь принадлежит к группе «Пользователи». Это локальная группа безопасности, членам которой разрешен доступ к ресурсам данного компьютера.

Диалоговое окно свойств позволяет настроить еще только те свойства учетной записи, которые имеют отношение к профилю (вкладка **Профиль**). Для изменения остальных свойств Windows XP Professional не предоставляет графического интерфейса.

Просмотреть и изменить свойства учетной записи можно по команде **net user**, которую нужно ввести в командной строке (набрав **cmd** в диалоговом окне **Выполнить** в меню **Пуск**). Команда **net user** без аргументов выведет список всех локальных учетных записей на этом компьютере. Команда **net help user** выведет краткую справку об использовании команды **net user** и свойствах учетной записи, которые можно настроить с ее помощью.

Если вы хотите просмотреть все свойства только что созданной записи, следует ввести в командной строке команду:

```
net user anvas
```

Вывод команды выглядит примерно следующим образом:

```
Имя пользователя                    Anvas
Имя и фамилия                       Васильев Андрей
Комментарий                         Начальник отдела продаж
Комментарий пользователя
Код страны                          000 (Стандартный системный)
Учетная запись активна              Да
Учетная запись просрочена           Никогда
Последний пароль задан              4.3.2005 1.45 PM
Действие пароля завершается         Никогда
Пароль допускает изменение          4.3.2005 1.45 PM
Требуется пароль                    Да
Пользователь может изменить пароль  Да
Разрешенные рабочие станции         Все
Сценарий входа
Конфигурация пользователя
Основной каталог
```

```
Последний вход                  Никогда
Разрешенные часы входа          Все
Членство в локальных группах    *Пользователи
Членство в глобальных группах   *Отсутствует
```

Ограничение срока действия учетной записи

Если созданная учетная запись принадлежит временному работнику, то вы можете задать дату, после которой эта запись станет недействительна:

```
net user anvas /expires:30.09.2005
```

При этом срок действия учетной записи закончится с началом суток 30 сентября 2005 года. Дату нужно вводить в кратком формате так, как это указано на вкладке **Региональные параметры** окна **Язык и региональные стандарты**.

Ограничение времени работы пользователя

Если предполагается, что новый пользователь будет работать за компьютером с 9 до 17 по рабочим дням и нет причин, по которым ему нужно было бы предоставить доступ к компьютеру вне этого времени, то вы можете указать время, в течение которого регистрация под данной учетной записью возможна:

```
net user anvas /times:Monday-Friday,9-17
```

Команда **net user anvas** отобразит сделанные вами изменения следующим образом:

```
Разрешенные часы входа      Понедельник 9.00 AM-5.00 PM
                            Вторник 9.00 AM-5.00 PM
                            Среда 9.00 AM-5.00 PM
                            Четверг 9.00 AM-5.00 PM
                            Пятница 9.00 AM-5.00 PM
```

Если пользователь попробует войти в систему вне указанного времени, то он увидит предупреждающее сообщение, а регистрация выполнена не будет.

Чтобы снять ограничения времени входа для этого пользователя, введите команду:

```
net user anvas /times:all
```

4.1.3. Вход в систему

Когда вы включаете компьютер с установленной на нем операционной системой Windows XP Professional, вы видите экран входа в систему, на котором каждая локальная учетная запись представлена значком и регистрационным именем. Чтобы зарегистрироваться в системе, нужно щелкнуть по значку и ввести пароль. Запустится процесс регистрации, по окончании которого перед пользователем появится его рабочий стол.

Такое положение дел представляет некоторый риск с точки зрения безопасности. Каждый, кто включит компьютер, увидит чужие учетные записи и, если ему повезет, сможет подобрать пароль и причинить неприятности законным пользователям. Скрыть регистрационные имена можно следующим образом:

1. Зарегистрируйтесь под именем Администратор.
2. Выберите в главном меню **Панель управления → Учетные записи пользователей**. Если вы переключили главное меню на классический вид, то папку **Панель управления** вы найдете в группе **Настройка**.
3. В диалоговом окне **Учетные записи пользователей** щелкните по ссылке **Изменение входа пользователей в систему**. Снимите флажок **Использовать страницу приветствия** и нажмите кнопку **Применение параметров**.
4. Выполните команду **Пуск → Выполнить** и в поле ввода введите команду **secpol.msc**. Откроется окно консоли **Локальные параметры безопасности**.
5. Разверните группу **Локальные политики** и выберите пункт **Параметры безопасности**.
6. В правой части окна консоли щелкните по пункту **Интерактивный вход в систему: не отображать последнего имени пользователя.** В появившемся окне свойств поставьте переключатель в положение **включен** и нажмите **OK**.

После этого экран приветствия вы больше не увидите. Вместо него будет отображаться стандартное окно входа, знакомое вам по предыдущим операционным системам семейства Windows NT.

Еще больше повысить безопасность входа в систему вы можете, заставив пользователя перед регистрацией нажимать комбинацию клавиш Ctrl+Alt+Del. Для этого на консоли **Локальные параметры безопасности** отключите режим **Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL.** Таким образом вы помешаете «работе» троянских коней, имитирующих диалог входа в систему с целью перехватить вводимые пользователем имя и пароль: если окно входа принадлежало посторонней программе, то нажатие Ctrl+Alt+Del вызовет перезагрузку и управление перейдет к настоящей операционной системе.

4.2. Разделение ресурсов

4.2.1. Общий доступ к папке

Войдя в систему, пользователь может запускать приложения, но не имеет права изменять параметры системы, если он не член группы «Администраторы».

С момента создания локальной учетной записи пользователи могут использовать ресурсы отдельного компьютера практически без ограничений. Но для полноценной работы этого недостаточно: рано или поздно им понадобится обмениваться документами с коллегами, работающими за другими компьютерами. Пользоваться дискетами или другими съемными носителями нецелесообразно, ведь у нас есть локальная сеть. Проще обеспечить доступ к общим папкам на сервере, в которые пользователь может поместить документы, предназначенные для коллег. Настроить разделение папки можно двумя способами, которые мы сейчас рассмотрим.

Менее безопасный способ

Менее безопасный способ выглядит следующим образом:

1. Зарегистрируйтесь на сервере SRVR001 под именем Администратор.
2. На диске D: создайте папку ABCD, а в ней — текстовый документ. Щелкните по значку папки правой кнопкой мыши и в контекстном меню выберите пункт **Общий доступ и безопасность**.
3. На вкладке **Доступ** (рис.4.2) установите флажок **Открыть общий доступ к этой папке** и в поле **Общий ресурс** введите имя, под которым эта папка будет известна в сети. Можете оставить имя ABCD.
4. Нажмите кнопку **Разрешения**. Убедитесь, что для группы пользователей «Все» («Everyone») установлен флажок доступа **Чтение/Разрешить.**
5. Закройте окно разрешений и в окне свойств разделяемой папки перейдите на вкладку **Безопасность**.
6. Нажмите кнопку **Добавить** и в появившемся окне выбора пользователей и групп, которым назначаются разрешения, введите «Everyone» (группа «Все»). Это должно быть имя существующей группы, поэтому его нужно набирать без опечаток: нажмите кнопку **Проверить имена.** Если вы не хотите вводить имя группы вручную, нажмите кнопку **Дополнительно**, чтобы выбрать его из списка. Добавив группу «Все», нажмите **ОК**. Закройте окно свойств папки ABCD.
7. Вызовите окно консоли **Управление компьютером**, в дереве консоли откройте объект **Локальные пользователи и группы → Пользователи.** В свойствах учетной записи «Гость» («Guest») снимите флажок **Отключить учетную запись**.

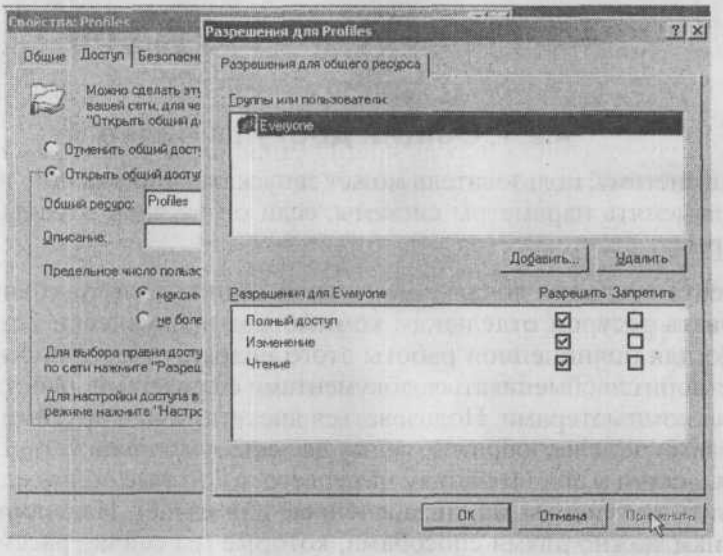


Рис. 4.2. *Свойства папки — назначение общего доступа*

Чтобы подключиться к разделенной папке с клиентского компьютера, зарегистрируйтесь на нем как обычный пользователь, выполните команду **Пуск → Выполнить** и в поле **Открыть** введите путь к общей папке: \\SRVR001\ABCD (если вы дали папке сетевое имя, то вместо ABCD наберите, естественно, его).

Более безопасный способ

Более безопасный способ реализуется следующей последовательностью действий:

1. Зарегистрируйтесь на сервере SRVR001 под именем Администратор.
2. Вызовите окно консоли **Управление компьютером**, откройте пункт **Локальные пользователи и группы → Пользователи.** В меню **Действие** выберите команду **Новый пользователь** и создайте учетную запись, полностью идентичную (включая пароль) локальной учетной записи того пользователя, которому вы хотите предоставить доступ к разделенной папке. Снимите флажок **Потребовать смену пароля при следующем входе в систему.**
3. На диске D: создайте папку BCDE, а в ней — текстовый документ. Щелкните по значку папки правой кнопкой мыши и в контекстном меню выберите пункт **Общий доступ и безопасность.**
4. На вкладке **Доступ** установите флажок **Открыть общий доступ к этой папке** и в поле **Общий ресурс** введите имя, под которым эта папка будет известна в сети. Можете оставить имя BCDE.

5. Перейдите на вкладку **Безопасность**. Удалите из списка разрешений группу «Все» («Everyone»). Вместо нее добавьте того пользователя, которому вы открываете доступ: нажмите кнопку **Добавить** и в появившемся окне введите его регистрационное имя. Можете выбрать его из списка, нажав кнопку **Дополнительно**. Нажмите **ОК** и закройте окно свойств папки BCDE.

Сравнение двух способов

Как обычно, за все нужно платить. Первый способ намного проще, когда требуется открыть доступ к папке не одному пользователю, а нескольким десяткам. Однако цена этой простоты — меньшая безопасность сетевой среды. Придется разрешить учетную запись «Гость» («Guest»), которая не требует ввода пароля, не только на всех рабочих станциях, но и на сервере, и под ней сможет зарегистрироваться кто угодно. Еще одно неудобство состоит в том, что все пользователи имеют одинаковый уровень доступа к папке (в нашем примере — только чтение), и их права невозможно дифференцировать.

Второй способ значительно безопаснее. Он основан на автоматическом сопоставлении регистрационных имен на удаленном компьютере и на том, который открывает доступ к ресурсу.

Если учетные записи (имя и пароль) совпадают, то доступ будет разрешен. Недостаток этого способа состоит в необходимости заводить локальные учетные записи для каждого пользователя, которому требуется открыть доступ к папке. С другой стороны, уровень доступа (запись, только чтение и т.д.) можно регулировать для каждого пользователя по отдельности.

Примечание.

При использовании автоматического сопоставления учетных записей необходимо поддерживать их в одинаковом состоянии на всех компьютерах, на которых пользователь имеет право регистрироваться. То есть если пользователь сменит пароль на одном компьютере, то он должен проделать это же и на всех остальных. В противном случае автоматическое сопоставление перестанет работать.

4.2.2. Печать на сетевых принтерах

Для печати на сетевых принтерах (то есть принтерах, подключенных к серверу печати, а не к локальному компьютеру) действуют те же правила, что и для доступа к сетевым папкам. Открыть доступ к принтеру можно теми же самыми двумя способами, причем первый из них можно рекомендовать только в среде, где не требуется практически никаких гарантий безопасности.

4.2.3. Работа с другими компьютерами.

Если пользователь собирается работать за другим компьютером, то безусловно необходимо, чтобы на этом компьютере для него была создана учетная запись. Сколько рабочих станций должно быть ему доступно, столько понадобится и учетных записей. Но тогда неразрешимым остается вопрос синхронизации смены пароля.

Дисциплинированный пользователь не только заводит себе «сильный» пароль, но и меняет его время от времени. Но сменить его он может только на том компьютере, за которым в данный момент работает. При этом перестанет работать автоматическое сопоставление учетной записи с учетными записями на других компьютерах, и разделяемые ресурсы, расположенные на них, перестанут быть этому пользователю доступны. Следовательно, ему придется обойти все компьютеры и сменить пароль на каждом, потратив на это немало времени.

4.3. Профили пользователей

При первой регистрации пользователя на компьютере для него создается локальный пользовательский профиль, то есть группа настроек, определяющих рабочую среду этого пользователя. Он включает помимо прочего следующие настройки:

- **Данные приложений**. Данные, сохраняемые отдельными приложениями, их настройки, журналы и временные файлы. Какая информация будет тут помещена, решают разработчики приложений.
- **Рабочий стол**. Все значки, размещенные на рабочем столе, то есть то, что пользователь видит перед собой.
- **Избранное**. Ссылки на любимые веб-страницы.
- **Документы**. Содержимое папок «Мои Документы» и «Недавние Документы».
- **Главное меню.** Содержимое группы «Все программы» в меню «Пуск».

Если вы создадите в компьютере учетные записи и не сконфигурируете их, то при первом входе пользователя на локальном диске в папке `%systemroot%\Documents and Settings\%username%` автоматически создастся профиль. Все изменения, вносимые в профиль, фиксируются на локальном диске. Если пользователь зарегистрируется на другом компьютере через локальную учетную запись на нем, то таким же образом создастся новый профиль. Если пользователю нужна одинаковая рабочая среда на всех компьютерах, то ему придется вручную настраивать ее на каждом.

Для облегчения миграции пользователей Windows XP Professional предоставляет возможность создания так называемого перемещаемого профиля. Такой профиль, однажды настроенный, будет действителен на любом компьютере, на котором зарегистрируется пользователь. При этом отпадает необходимость согласовывать локальные профили. Перемещаемый профиль должен быть доступен с любого компьютера при каждой регистрации, поэтому его следует разместить на постоянно работающем сервере.

Работа с перемещаемыми профилями и возникающие при этом проблемы подробно описаны в главе 13.

В нашей сетевой среде настройка перемещаемых профилей состоит из следующих шагов:

1. Создание на постоянно доступном сервере разделяемой папки, в которую будут помещены профили.
2. Конфигурирование пользовательских учетных записей.
3. Создание перемещаемого профиля.

Создание сетевой папки для помещения в нее профилей

1. Зарегистрируйтесь на сервере SRVR001 как Администратор.
2. На диске D: создайте папку `Profiles` (Профили). Откройте к ней общий доступ и дайте группе «Все» («Everyone») разрешение NTFS «Полный доступ» (рис.4.2, вкладка **Безопасность** в окне свойств папки Profiles).

Конфигурирование пользовательских учетных записей

Учетная запись пользователя, которому требуется перемещаемый профиль, должна присутствовать на каждом компьютере, за которым он собирается работать. Эту учетную запись нужно настроить следующим образом:

1. В окне консоли **Управление компьютером** раскройте объект **Локальные пользователи и группы Пользователи.**
2. Для каждого пользователя в свойствах учетной записи укажите в поле **Профиль** путь к сетевой папке: `\\SRVR001\profiles\%username%`. Закройте окно свойств учетной записи нажатием кнопки **OK**.

Примечание.

Вместо системной переменной `%username%` можно указать и конкретное регистрационное имя пользователя. Переменную выгоднее использовать тогда, когда вы настраиваете несколько учетных записей сразу при помощи командного сценария.

Создание перемещаемого профиля

Для создания перемещаемого профиля нужно выполнить следующую последовательность действий:

1. Зарегистрируйтесь на рабочей станции с операционной системой Windows XP Professional как Администратор.
2. Заведите временную учетную запись (с ограниченным сроком действия). Она понадобится для создания локального профиля — шаблона для новых пользователей.
3. Перерегистрируйтесь под только что созданной учетной записью. При первом входе в систему будет автоматически создан локальный профиль. Настройте его в соответствии с вашими требованиями (можете, например, добавить ярлыки на рабочий стол, установить сетевые принтеры или настроить главное меню) и завершите сеанс работы.
4. Снова зарегистрируйтесь как Администратор. В главном меню щелкните правой кнопкой мыши по иконке **Мой компьютер** и выберите из контекстного меню команду **Свойства**.
5. На вкладке **Дополнительно** нажмите кнопку **Параметры** в области **Профили пользователей**. Выберите из списка профиль временной учетной записи и нажмите кнопку **Копировать**.
6. В поле **Копировать профиль на** введите полный путь к профилю того пользователя, для которого вы настраиваете перемещение, на сервере: `\\SRVR001\Profiles\anvas`.
7. В области **Разрешить использование** нажмите кнопку **Изменить** и введите регистрационное имя того пользователя, для которого настраиваете профиль: anvas.
8. Нажмите **ОК**. Операционная система Windows XP Professional создаст в папке `\\SRVR001\Profiles` подпапку `anvas` и предоставит полный доступ к ней пользователю `anvas` и группе «Администраторы».

Перемещаемый профиль для уже существующего пользователя создается так же, только в качестве шаблона следует использовать существующий локальный профиль этого пользователя.

Если вы хотите создать перемещаемый профиль для уже существующего пользователя, вам нужно будет совершить те же действия с той, однако, разницей, что вам не надо создавать временного пользователя и его профиль, а просто достаточно просто копировать актуальные учетные данные пользователя с компьютера, на котором пользователь работает.

Дальнейшие сведения о профилях вы найдете в 13 главе.

Примечание.

В сетевой среде, работающей исключительно под ОС Windows 2000, использование перемещаемых профилей не рекомендуется.

4.4. Домашние папки

Вы можете посчитать, что для вашей сетевой среды применение перемещаемых профилей слишком сложно и непрактично. Более экономным решением было бы организовать для пользователей доступ к папке с их документами с любой рабочей станции.

Папка, по умолчанию предназначенная для документов пользователя, называется его домашней папкой. У пользователя с локальным профилем это папка **Мои документы**, расположенная на локальном диске и доступная с другой рабочей станции только тогда, когда включена эта. Чтобы документы пользователя были доступны в любое время с любого компьютера сети, нужно хранить их на сервере. Это выгодно еще и потому, что резервное копирование данных на сервере происходит регулярно, а на рабочей станции это зависит от дисциплины пользователя.

В сети, где клиентские компьютеры работают под управлением Windows XP Professional, организовать домашнюю папку пользователя на сервере можно следующим образом:

1. На всех рабочих станциях и на сервере заведите пользовательские учетные записи с одним и тем же регистрационным именем и паролем.
2. На сервере SRVR001 создайте на диске C: папку `Documents`. Откройте общий доступ к этой папке и дайте группе «Все» («Everyone») разрешение **Изменение** (**Modify**).
3. На каждом компьютере измените учетную запись так, чтобы она указывала на дочернюю папку `Documents` в качестве домашней папки: откройте окно свойств учетной записи, перейдите на вкладку **Профиль**, в области **Домашняя папка** поставьте переключатель в положение **Подключить**, выберите букву диска (рекомендуем оставить Z:) и в поле **На** введите полный путь к личной подпапке пользователя в общей папке `Documents`: `\\SRVR001\Documents\%username%`. По нажатии кнопок **ОК** или **Применить** в папке Documents на сервере будет создана подпапка с именем, совпадающим с регистрационным именем пользователя. Доступ к ней пока настраивать не нужно.

Теперь, зарегистрировавшись на любом компьютере сети, пользователь получит в распоряжение диск Z: и выбор, где ему сохранять важные документы: на Z: или, как обычно, в локальной папке **Мои документы**. Если вы считаете, что предоставлять такой выбор нежелательно, потому что его наличие только собьет пользователя с толку, то можно вручную перенаправить папку **Мои документы** в домашнюю папку (диск Z:). Откройте окно свойств папки **Мои документы**, перейдите на вкладку **Папка назначения** и в поле **Папка** укажите путь к домашней папке: Z:.

Недостатком этого простого решения является то, что все пользователи получают доступ к домашним папкам друг друга. Если это не входит в

ваши намерения, то для домашних папок нужно соответствующим образом настроить разрешения NTFS:

1. Откройте окно свойств папки `%username%` (домашней папки конкретного пользователя на сервере).
2. Перейдите на вкладку **Безопасность** и нажмите кнопку **Дополнительно**. Снимите флажок **Наследовать от родительского объекта**, нажмите кнопку **Копировать**, а затем **OK**.
3. Из списка пользователей и групп, для которых определены права доступа к домашней подпапке, удалите группу `SRVR001\Users` и добавьте вместо нее конкретного пользователя. Назначьте ему разрешение **Изменение** (**Modify**).
4. Закройте окно свойств папки нажатием кнопки **OK**.

Теперь можно убедиться в том, что ни один обычный пользователь не имеет доступа к домашней папке другого и тем самым пользователи получили безопасный и мобильный в пределах сети доступ к своим документам.

4.5. Итоги

Чтобы пользователь мог зарегистрироваться на компьютере, входящем в рабочую группу, он должен иметь на этом компьютере учетную запись. Основные свойства локальной учетной записи можно настроить через графический интерфейс. Для настройки остальных свойств (например, времени действия учетной записи или часов разрешенного доступа) служит команда **net user**.

Самый безопасный способ входа пользователей в систему — через нажатие комбинации клавиш Ctrl+Alt+Del. Если этот способ не настроен, а используется, например, экран приветствия, то посторонний видит регистрационные имена всех законных пользователей и может, подобрав пароль, зарегистрироваться под именем одного из них.

Чтобы обеспечить нескольким пользователям совместный доступ к документам, нужно создать на постоянно работающем сервере разделяемую (общую) папку. Права доступа к ней можно настроить двумя способами. Первый, менее трудоемкий и менее безопасный, — разблокировать гостевую учетную запись («Guest») и открыть доступ всем. Второй — предоставить доступ каждому пользователю индивидуально. Точно так же организуется совместный доступ к сетевым принтерам.

При первой регистрации пользователя на рабочей станции создается его профиль, то есть совокупность настроек его личного рабочего пространства, изолированных от настроек других пользователей. В профиль

входит домашняя папка пользователя, предназначенная для размещения его личных документов. Если локальный жесткий диск в компьютере отформатирован файловой системой NTFS, то профиль создается с такими разрешениями NTFS, что доступ к нему разрешен только владельцу и Администратору. Такой профиль называется локальным.

Если пользователю нужно работать за разными компьютерами, то можно сделать так, чтобы на них всех использовался один и тот же профиль. Такой профиль называется перемещаемым, и его настройка была описана выше. Домашняя папка, входящая в состав профиля, при использовании перемещаемых профилей становится доступна пользователю с любого компьютера. В небольшой сети настройка перемещаемых профилей может оказаться излишне трудоемкой и можно ограничиться локальными профилями, разместив на сервере только домашнюю папку. Эта домашняя папка будет доступна пользователю с рабочей станции как новый диск, и он сможет выбирать, где хранить свои данные: на нем или в папке **Мои документы**.

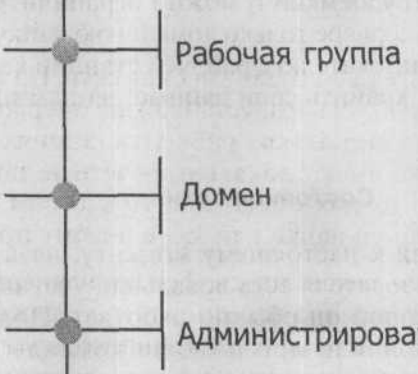
Состояние сети

Модель сети, развернутая к настоящему моменту, называется рабочей группой. У каждого пользователя есть локальная учетная запись на той рабочей станции, за которой он обычно работает. Полную настройку учетной записи мы выполнили при помощи команды **net user**. Если пользователю требуется работать за несколькими компьютерами, то на каждом из них созданы одинаковые учетные записи (использование гостевой учетной записи не рекомендуется с точки зрения безопасности). Для размещения документов пользователей мы выбрали одну из следующих моделей:

- Перемещаемый профиль.
- Локальный профиль и сетевая домашняя папка.

Поскольку администрирование перемещаемых профилей — процесс достаточно трудоемкий и в среде рабочей группы не окупающийся, мы рекомендуем использовать вторую модель. На сервере к этому моменту могут существовать разделяемые папки `Profiles` и `Documents`.

Глава 5 Сеть растет. Структурирование растущей сети



К этому моменту у нас есть небольшая учебная сеть. На компьютере, который будет исполнять роль сервера, установлена операционная система Windows Server 2003, а на нескольких рабочих станциях — Windows XP Professional. Пользователи имеют локальные учетные записи на каждом компьютере и с каждого из них имеют доступ к своим данным, хранящимся на сервере: домашней папке или даже целому профилю.

На этом все, что попроще, закончилось. Теперь начинаются трудности. Сеть такой структуры совершенно невозможно поддерживать при увеличении числа пользователей. Кроме того, администрирование такой сети требует глубокого знания конкретных нужд пользователей.

Возможности администраторов весьма различны. Один может эффективно управлять только такой сетевой средой, в которой работает десяток-другой компьютеров, для другого не проблема и сотня. Подходы к управлению сетью у них разные, и мало в чем они друг с другом согласятся. Однако с ростом сети рано или поздно наступит момент, когда оба они скажут, что так дальше уже нельзя.

В этой главе мы рассмотрим и сравним различные возможности структурирования растущей сети.

5.1. Рабочая группа

В ходе установки системы вы оставили в диалоговом окне **Рабочая группа или домен компьютера** значение по умолчанию: рабочую группу с именем WORKGROUP (ГРУППА).

Рабочую группу, называемую также сетью peer-to-peer или одноранговой сетью равноправных пользователей, отличают следующие основные характеристики.

- Рабочая группа — это простое и дешевое решение задачи объединения в сеть небольшого количества пользователей.
- В сети типа «рабочая группа» все узлы равноправны и находятся на одном и том же уровне. Узлы не имеют возможности эффективно сотрудничать, и не существует простого способа их единообразно администрировать.
- Каждый пользователь должен иметь учетную запись на каждом из компьютеров, за которыми ему нужно работать.
- Учетные записи пользователей хранятся на локальном компьютере в базе данных системы безопасности (SAM, Security Account Manager).
- Чтобы работать с ресурсами удаленного компьютера, пользователь должен иметь на нем учетную запись с тем же регистрационным именем и паролем, что на локальном компьютере. В противном случае при каждом обращении к сетевому ресурсу ему придется заново вводить имя и пароль.
- Если пользователь захочет сменить пароль, он должен будет сделать это на всех узлах, где у него имеется учетная запись. Если он этого не сделает, он потеряет прямой доступ к разделяемым ресурсам, расположенным на других узлах.
- Любые настройки безопасности, выполненные с консоли **Локальные параметры безопасности**, действительны только на локальном компьютере.

Рабочая группа — это структура, предназначенная для малых сетей (до десятка компьютеров), когда пользователи объединяются для того, чтобы иметь доступ к сетевым ресурсам, таким как разделяемые папки или сетевые принтеры.Может показаться, что такая структура скорее бесполезна, чем выгодна, но у нее есть определенные преимущества. Рабочую группу легко администрировать, и справиться с ней может администратор минимальной квалификации.

А для крупной и развивающейся сети придется найти модель получше. От этой модели требуется удобство управления пользовательскими учетными данными и другими характеристиками сети и масштабируемость, то есть независимость принципов ее работы от количества узлов в сети. Такой моделью является домен.

5.2. Домен

Домен можно рассматривать как логическую группу объектов сети. Под объектами понимаются компьютеры, учетные записи, группы пользователей и т. д.

Как можно охарактеризовать домен по сравнению с рабочей группой?

- Узлы в домене иерархически упорядочены. На верху иерархии находится компьютер, на котором размещена доменная база данных, т. н. контроллер домена.
- Пользователь имеет лишь одну, т.н. «доменную», учетную запись, под которой он может регистрироваться на любом компьютере, входящем в домен.
- Учетная запись пользователя находится в базе данных домена. Базой данных домена управляет контроллер домена. Если компьютеров, выполняющих функции контроллера домена, несколько, то они время от времени синхронизируют свои доменные базы данных — на тот случай, если какой-нибудь из них выйдет из строя или если в сети много пользователей и один контроллер домена не справился бы с таким количеством.
- Доступ к ресурсам других компьютеров в домене управляется доменной учетной записью пользователя. Локальные учетные данные в домене не нужны.
- Если пользователь меняет пароль, то изменяется его доменная учетная запись. С новым паролем он может регистрироваться на любом компьютере домена.
- Безопасность можно настроить для всего домена сразу при помощи групповых политик.

Доменная модель — единственный разумный выбор для сетей среднего и большого размеров. Она предоставляет возможности для более эффективного управления, обеспечивает большую безопасность окружения и в результате снижает расходы на вычислительную технику.

5.3. Администрирование домена

По сравнению с рабочей группой управление доменом на первый взгляд выглядит гораздо сложнее, но оно предоставляет и больше возможностей. Само собой, нельзя сразу стать полноценным администратором домена, потому что каждую из его функций нужно хорошо понять и научиться ею пользоваться. Чтобы эффективно администрировать домен, вам потребуется и хорошая теоретическая подготовка, и практические навыки. Надо заметить, что в литературе об этом иногда можно встретить ошибки, так что способность администрирования сети приходит еще и с опытом.

Если вы будете знать возможности доменной среды, уметь настраивать и использовать ее, ваша работа станет намного проще и эффективнее.

На практике довольно часто встречается ситуация, когда администраторы домена не знают как следует свойств и функций доменной среды или не умеют их применить и покупают новое программное обеспечение или

даже новое оборудование для решения тех задач, для которых и предназначены функции домена. Таким образом не только тратятся лишние средства, но и администраторы добавляют себе хлопот по обслуживанию установленных приложений, что тоже увеличивает расходы на управление сетью.

5.4. Итоги

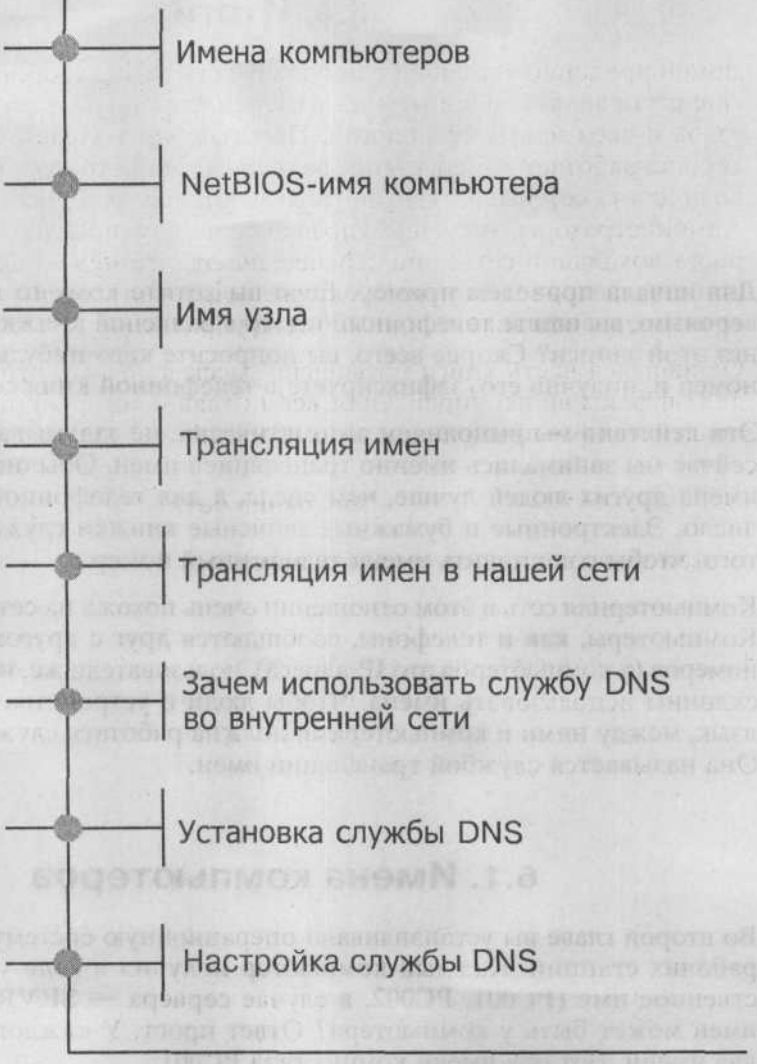
Домен представляет собой единую область сети, которой можно эффективно управлять, несмотря на изменение условий работы, рост числа узлов и ввод новых технологий. Простым показателем того, насколько хорошо работает домен, станет реакция администраторов на увеличение количества сетевых объектов (пользователей, рабочих станций и т.п.). Администраторы, уверенно управляющие доменом, не должны бояться роста локальной сети: они заранее знают, что нужно сделать. Если же администратора пугает рост окружения, значит, он не обладает достаточным запасом знаний или запустил управление сетью.

Оставшаяся часть книги посвящена рассказу о том, что нужно сделать для эффективного управления всеми главными функциями домена, и практическому применению этих функций.

Состояние сети

В этой главе состояние сети не изменилось.

Глава 6 Для чего и как в сети преобразуюся имена



Для начала приведем пример. Если вы хотите кому-то позвонить, то, вероятно, вы ищете телефонный номер в записной книжке. А если у вас нет этой записи? Скорее всего, вы попросите кого-нибудь дать вам этот номер и, получив его, зафиксируете в телефонной книжке.

Эти действия мы выполняем автоматически, не задумываясь о том, что сейчас мы занимались именно трансляцией имен. Обычно люди помнят имена других людей лучше, чем числа, а для телефонной связи нужно число. Электронные и бумажные записные книжки служат как раз для того, чтобы сопоставить имени телефонный номер.

Компьютерная сеть в этом отношении очень похожа на сеть телефонную. Компьютеры, как и телефоны, сообщаются друг с другом посредством номеров (у компьютеров это IP-адреса), пользователи же, наоборот, более склонны использовать имена. Чтобы люди и устройства нашли общий язык, между ними и компьютерами должна работать служба-посредник. Она называется службой трансляции имен.

6.1. Имена компьютеров

Во второй главе вы устанавливали операционную систему на несколько рабочих станций. Каждый компьютер получил в ходе установки собственное имя (PC001, PC002, в случае сервера — SRVR001). Сколько имен может быть у компьютера? Ответ прост. У каждого компьютера два имени. Вот оба имени компьютера PC001:

1 имя — PC001
2 имя — PC001

С одной стороны, наличие у компьютера двух вроде бы одинаковых имен выглядит несколько странным. Однако они служат совершенно различным целям.

Компьютер (или другое устройство) является узлом сети, и первое из названных имен — это имя узла (рис. 6.1).

Второе из названных имен — так называемое имя интерфейса NetBIOS (Network Basic Input/Output System) (см. рис. 6.2). NetBIOS — это программный интерфейс для приложений типа клиент-сервер.

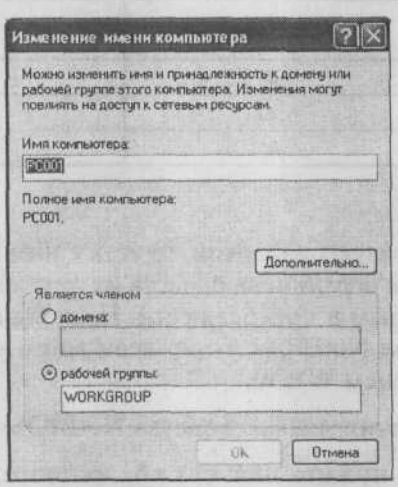


Рис. 6.1. *В поле* ***Имя компьютера*** *вписано имя узла*

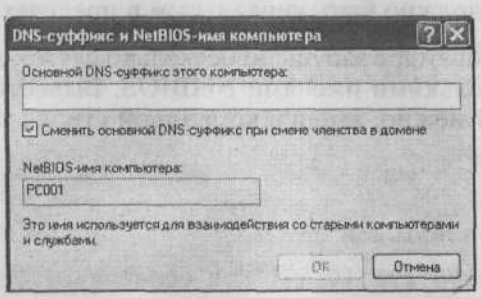


Рис. 6.2. *NetBIOS-имя компьютера*

6.2. NetBIOS-имя компьютера

NetBIOS-имя — это идентификатор, который используют службы, работающие на данном компьютере по протоколу NetBIOS. Он служит для однозначной идентификации узла в сети NetBIOS. Длина этого имени составляет 16 байтов, где первые 15 — обычные печатные символы, а шестнадцатый байт идентифицирует службу, запущенную на компьютере (табл. 6.1).

Примеры имен NetBIOS *Таблица 6.1*

Имя NetBIOS	16-й байт	Служба
SRVR001	00	Workstation
SRVR001	20	Server
SRVR001	01	Messenger

Имена NetBIOS не образуют иерархии, то есть к ним нельзя дописать никаких суффиксов. Этим ограничена область их применения: имя NetBIOS должно быть уникальным в пределах сети. Если бы в основу Интернета был положен протокол NetBIOS, то во всем мире мог бы быть только один компьютер с именем WWW.

Из этого следуют отличительные свойства NetBIOS-имен:

- Имена NetBIOS нужны для служб, использующих интерфейс NetBIOS. Службы, встроенные в операционные системы Windows 2000 и Windows XP Professional, не используют этого интерфейса, однако, если в сети есть компьютеры с предыдущими версиями операционных систем Windows, то в пределах сети должна работать служба трансляции имен NetBIOS.
- Имя NetBIOS не обязано совпадать с именем узла.
- Имя NetBIOS должно быть уникальным в пределах сети.

Если на одном компьютере запущено несколько служб, то в сети он будет известен под несколькими именами NetBIOS. Вывести список локальных имен NetBIOS можно, введя в командной строке команду команды **nbtstat –n**:

```
C:\>nbtstat -n
Подключение по локальной сети:
Адрес IP узла [168.192.10.17] Код области: [ ]
```

```
Локальная таблица NetBIOS-имен
Имя                 Тип             Состояние
PC001       <00>    Уникальный      Зарегистрирован
WORKGROUP   <00>    Группа          Зарегистрирован
PC001       <20>    Уникальный      Зарегистрирован
PC001       <03>    Уникальный      Зарегистрирован
WORKGROUP   <1E>    Группа          Зарегистрирован
WORKGROUP   <10>    Уникальный      Зарегистрирован
..__MSBROWSE__ <01> Группа          Зарегистрирован
```

6.3. Имя узла

Имя узла однозначно идентифицирует компьютер или устройство. По этому имени узел можно найти в Интернете, потому что имена узлов образуют иерархическую систему. Полное доменное имя (FQDN, Full Qualified Domain Name), уникальное в пределах Интернета, образуется соединением имени узла и так называемого суффикса DNS (рис.6.3). Это значит, что несколько узлов в сети могут иметь одно и то же имя, если они отличаются суффиксом DNS.

Например, полное доменное имя нашего сервера `SRVR001.study.local` состоит из двух частей: SRVR001 — имя узла, а `study.local` — суффикс. Где-нибудь в Интернете может встретиться имя `SRVR001.another-domain.com`, отличающееся от нашего только суффиксом.

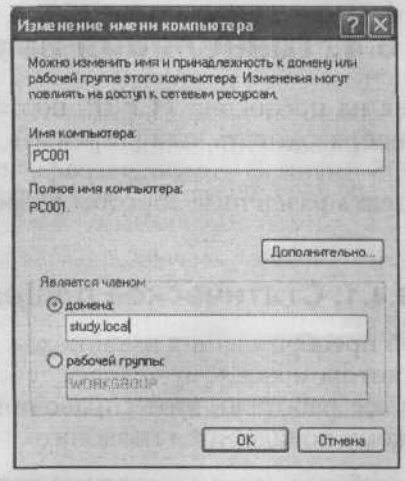


Рис. 6.3. *Имя узла, имя домена и полное доменное имя*

Вероятность встретить в Интернете имя узла SRVR001 не так уж велика. Но если вы вместо него дадите компьютеру имя WWW, то, пожалуй, вероятность встретить «тезку» резко возрастет.

Имя узла задается при установке операционной системы. Суффикс добавляется либо автоматически при установке, если компьютер является членом домена, либо указывается вручную потом.

Имена узлов отличаются следующими свойствами:

- Имя узла служит для идентификации компьютера или другого устройства в сети, работающей по протоколу TCP/IP.
- Имя узла не обязано совпадать с именем интерфейса NetBIOS.
- Максимальная длина имени узла — 63 символа.
- Один узел может быть известен в сети под несколькими именами.

На компьютере с операционной системой Windows XP Professional (Windows 2000 Professional) имя узла можно вывести с помощью утилиты командной строки HOSTNAME:

```
C:\hostname
pc001
```

Операционная система Windows 2000 и более новые используют по умолчанию имя узла, поэтому может показаться, что не стоит забивать себе голову еще и именами NetBIOS. Однако сети, где не найдется хотя бы одного компьютера с Windows предыдущей версии, встречаются пока редко. Поэтому в целях совместимости не стоит забывать об именах NetBIOS и их трансляции.

6.4. Трансляция имен

Наша сеть основана на протоколе TCP/IP, поэтому для ее работы необходимо уметь преобразовывать, или разрешать, в IP-адреса как имена узлов, так и NetBIOS-имена. В этом параграфе мы рассмотрим, а затем попробуем осуществить различные способы разрешения имен.

6.4.1. Статическое решение

Статический способ преобразования имен похож на печатный телефонный справочник, в котором каждому человеку сопоставлен его телефонный номер. Чтобы все работало, этот справочник должен быть всегда доступен любому, кому понадобится позвонить.

Далее ответим на наиболее часто задаваемые вопросы по статическому способу преобразования имен:

- **Как это работает в сети?** Каждый компьютер, который должен установить связь с другим по имени, полученному от пользователя или приложения, должен иметь доступ к таблице, в которой прописаны это имя и соответствующий ему IP-адрес.
- **Каковы недостатки статического решения?** Недостаток этого решения виден сразу: если IP-адрес в таблице написан с ошибкой, то связь не будет установлена. Такие ситуации могут возникать часто: смена IP-адреса в сетях с протоколом TCP/IP — обычное дело. Подумайте, при каком размере сети вы перестанете справляться с поддержанием таблиц преобразования имен в рабочем состоянии.
- **Каковы преимущества статического решения?** Естественно, статическое решение имеет и свои преимущества. Главное из них заключается в том, что, придерживаясь его, вы избавляетесь от необходимости устанавливать, настраивать и поддерживать сетевые службы, которые решали бы задачу трансляции имен другим способом.
- **Где статическое решение выгоднее других?**
  - В малой сети, работающей по протоколу TCP/IP.
  - В сети, где нет возможности настроить другие службы трансляции имен.
  - На отдельном компьютере, который подключается к сети удаленно и должен взаимодействовать только с несколькими ее узлами.

Статическая трансляция имен NetBIOS

Для преобразования имен NetBIOS в ОС Windows служит файл LMHOSTS. Для того, чтобы этот файл участвовал в процессе трансляции имен, должны быть выполнены следующие условия:

- Он должен иметь имя LMHOSTS (без расширения).
- Он должен находиться в папке `%systemroot%\system32\drivers\etc`.
- Он должен содержать необходимые строки.
- В окне настройки TCP/IP, на вкладке WINS, должен быть установлен флажок **Включить просмотр LMHOSTS** (рис. 6.4).

Файл LMHOSTS — это текстовый файл примерно следующего содержания:

```
192.168.10.2 SRVR001
192.168.10.17 PC001
192.168.10.18 PC001
```

Каждая строка этого файла сопоставляет IP-адресу единственное имя NetBIOS.

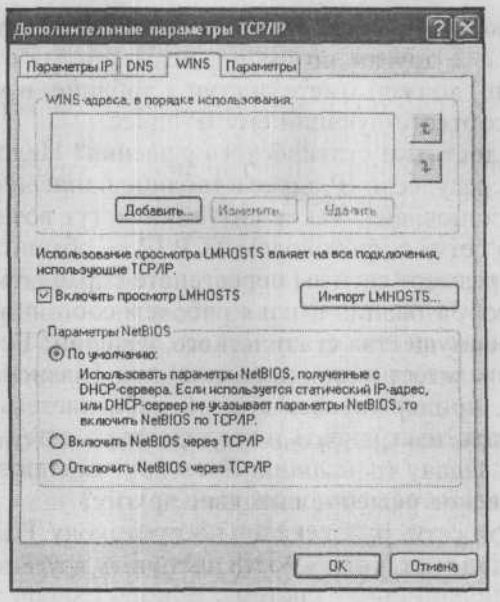


Рис. 6.4. *Включение просмотра LMHOSTS*

Статическая трансляция имен узлов

Для преобразования имен узлов в ОС Windows служит файл HOSTS. Для того, чтобы этот файл участвовал в процессе трансляции имен, должны быть выполнены следующие условия:

- Он должен иметь имя HOSTS (без расширения).
- Он должен находиться в папке `%systemroot%\system32\drivers\etc`.
- Он должен содержать необходимые строки.

Файл HOSTS — это текстовый файл примерно следующего содержания:

```
192.168.10.2 SRVR001 SRVR001.ourcompany.com SRVR.study.local
192.168.10.16 PC001 PC001.ourcompany.com
192.168.10.17 PC002 PC002.ourcompany.com PC002.study.local
```

Разницу между файлами HOSTS и LMHOSTS видно с первого взгляда. Каждая строка файла HOSTS может сопоставлять единственному IP-адресу несколько имен узлов либо полных доменных имен.

6.4.2. Динамическая трансляция имен

Пусть на предприятии есть список нужных телефонов. Есть два способа сделать его доступным для всех сотрудников. Первый — раздать копии, отпечатанные на бумаге, или разослать их по электронной почте. Второй —

разместить этот список на сервере и открыть всем доступ на просмотр (например, через Интернет).

Выгодность второго способа становится очевидной, когда в списке что-то меняется: достаточно исправить список один раз, чтобы все пользователи увидели новую информацию. Первый способ намного более трудоемок, поскольку он требует повторной рассылки исправленного списка и контроля за тем, чтобы пользователи его получили и приняли к сведению.

Вы уже, вероятно, заметили, что первый способ приведен как аналогия статического решения, о котором только что шла речь. Второй же способ — база данных, к которой имеют доступ все, кому она требуется, — аналогичен динамическому решению, которое мы рассмотрим сейчас.

Динамическая трансляция имен NetBIOS

Имена NetBIOS и соответствующие им IP-адреса хранятся в базе данных службы WINS (Windows Internet Name Service). База данных WINS должна быть размещена на сервере WINS, а сервер WINS можно установить как компонент операционной системы Windows Server 2003 или Windows 2000 Server. Это значит, что в сети должен быть хотя бы один компьютер с серверной операционной системой, иначе динамическое решение использовать невозможно.

Далее ответим на общие вопросы по динамической трансляции имен NetBIOS:

- **Как имена и IP-адреса попадают в базу WINS?** Каждый компьютер, являющийся клиентом WINS (то есть имеющий доступ к серверу WINS по его IP-адресу) при включении регистрирует на этом сервере все свои имена NetBIOS. После регистрации они и IP-адрес зарегистрировавшего их узла становятся доступны для любого узла сети.
- **Что делать, если компьютер не может зарегистрировать свои NetBIOS-имена?** В распоряжении администратора есть возможность занести в базу IP-адрес и соответствующие ему NetBIOS-имена вручную, создав таким образом статический список, который нельзя удалить иначе, чем вручную. Не забывайте контролировать правильность статического списка, а в случае изменений своевременно вносить в него поправки.
- **Как поддерживать базу в актуальном состоянии?** При выключении клиент WINS посылает серверу WINS запрос на освобождение списка. При следующем включении компьютер заново регистрирует свои имена NetBIOS с тем IP-адресом, который у него окажется на этот момент.
- **Что произойдет, сеанс работы компьютера завершится аварийно и запрос на освобождение списка не будет послан или сервер WINS в этот момент окажется недоступен?** Ничего страшного. Если у сервера WINS есть база активных имен NetBIOS и пришел запрос на регистрацию

тех же имен, он проверит соответствующий им IP-адрес с помощью утилиты PING. Если текущий список еще действителен (IP-адрес не изменился), то запрос на перерегистрацию клиента будет отклонен.

Как уже было сказано, система Windows 2000 и более новые работают преимущественно с именами узлов.

Динамическая трансляция имен узлов

Имена узлов и соответствующие им IP-адреса хранятся в базе данных службы DNS (Domain Name System). Служба DNS управляет иерархически организованным пространством имен и хранит информацию в так называемых зонах. Организовать хранение зон DNS можно разными способами: поместить их как файлы на сервер, где запущена служба DNS, или включить в доменную базу данных. Важно помнить, что каждой зоне соответствует один файл (в том случае, если зоны хранятся как файлы). Службу DNS можно установить как компонент операционной системы Windows 2000 Server или Windows Server 2003.

Далее ответим на общие вопросы по динамической трансляции имен узлов на основе базы DNS:

- **Как имена узлов и IP-адреса попадают в базу DNS?** Компьютеры с ОС Windows XP Professional или Windows 2000 Professional способны автоматически зарегистрировать свое имя узла и IP-адрес в базе данных службы DNS. После регистрации эти данные становятся доступны всем узлам сети.
- **Что делать, если компьютер не может зарегистрировать свое имя узла?** В таком случае есть две возможности:
- Внести соответствующую запись (или несколько записей, если у компьютера несколько IP-адресов) в базу данных DNS вручную.
- Если для раздачи IP-адресов в сети служит сервер DHCP (входящий в состав ОС Windows Server 2003 и Windows 2000 Server), можно настроить его так, чтобы он проводил эту регистрацию за клиентов. Эта возможность особенно полезна, если в сети работают клиентские компьютеры с ОС Windows 95, 98, NT 4.0 и т.п.
- **Как поддерживать базу в актуальном состоянии?** Клиентские компьютеры не посылают при выключении никакого запроса на освобождение своей записи. Об ее удалении сервер DNS должен позаботиться сам. Эта функция бывает настроена не всегда, но даже так — ничего страшного нет. При включении клиент регистрируется с новым IP-адресом, и в зоне появляются две записи: с одним именем узла, но с разными IP-адресами. Трансляции имен это не повредит.

Поскольку операционные системы семейства Windows 2000 и более новые работают с именами узлов, стоит подумать о том, чтобы установить службу DNS для их трансляции.

6.5. Трансляция имен в нашей сети

Устанавливая серверную ОС, мы не установили ни сервера WINS, ни DNS. Поэтому единственными параметрами протокола TCP/IP, которые мы настраивали на рабочих станциях, был IP-адрес и маска подсети. Мы не указывали IP-адресов служб WINS и DNS. Посмотрим, как при таких условиях транслируются имена.

6.5.1. Имена узлов

Преобразование имен узлов лучше всего можно продемонстрировать с помощью утилиты PING.

1. Зарегистрируйтесь на PC001 как Администратор.
2. Введите команду **ping srvr001**. Вы увидите что-то вроде этого:

```
C:\>ping srvr001
Обмен пакетами с srvr001 [192.168.10.2] по 32 байт:
Ответ от 192.168.10.2: байты=32 время=2мс TTL=128
Ответ от 192.168.10.2: байты=32 время<1мс TTL=128
Ответ от 192.168.10.2: байты=32 время<1мс TTL=128
Ответ от 192.168.10.2: байты=32 время<1мс TTL=128
Статистика ping для 192.168.10.2:
Пакетов: отправлено=4, получено=4, потеряно=0 (0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

3. Теперь зарегистрируйтесь на SRVR001 как Администратор.
4. Введите команду **ping pc001**. Ответ будет следующим:

```
C:\>ping pc001
Обмен пакетами с pc001 [192.168.10.17] по 32 байт:
Ответ от 192.168.10.17: байты=32 время<1мс TTL=128
Ответ от 192.168.10.17: байты=32 время<1мс TTL=128
Ответ от 192.168.10.17: байты=32 время<1мс TTL=128
Ответ от 192.168.10.17: байты=32 время<1мс TTL=128
Статистика ping для 192.168.10.17:
Пакетов: отправлено=4, получено=4, потеряно=0 (0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

6.5.2. Имена NetBIOS

Трансляцию имен NetBIOS мы проверим при помощи UNC-путей.

1. Зарегистрируйтесь на PC001 как Администратор.

2. Выполните команду **Пуск → Выполнить** и в поле **Открыть** укажите UNC-путь к серверу: \\SRVR001. Вы увидите окно со значками разделяемых ресурсов на сервере SRVR001 (рис. 6.5).
3. Зарегистрируйтесь на SRVR001 как Администратор.
4. Выполните команду **Пуск → Выполнить** и в поле **Открыть** укажите UNC-путь к компьютеру PC001: \\PC001. Если появится диалоговое окно с запросом пароля для гостевой учетной записи («Guest») на компьютере PC001, то запустите на PC001 **Проводник Windows** и в меню **Сервис** выберите пункт **Свойства папки**. Затем на вкладке **Вид** снимите флажок **Использовать простой общий доступ к файлам (рекомендуется)**. Вы должны увидеть окно со значками разделяемых ресурсов на PC001 (рис. 6.6).

Что происходит? Мы не устанавливали ни службу WINS, ни DNS, не редактировали файлов HOSTS и LMHOSTS ни на одном из компьютеров, однако они прекрасно находят друг друга в сети по именам. Чтобы понять этот процесс, нужно знать последовательность действий компьютера по разрешению имен. Если в сети работает сервер WINS, а на локальном компьютере настроен просмотр LMHOSTS, то который из способов трансляции имен будет применен в первую очередь? Тот же

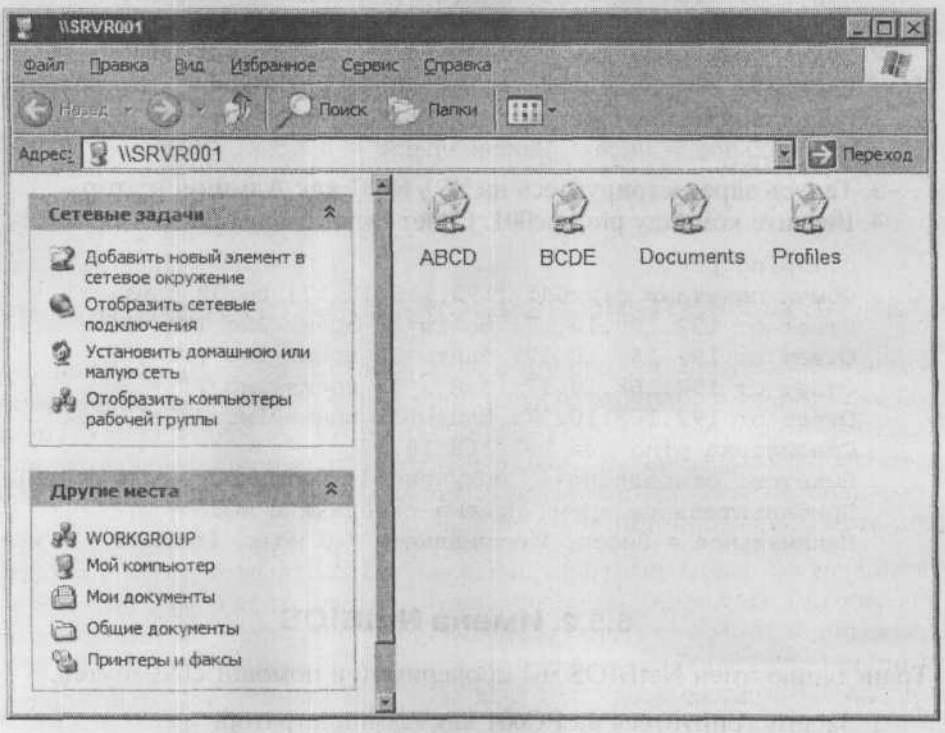


Рис. 6.5. *Разделяемые ресурсы на сервере SRVR001*

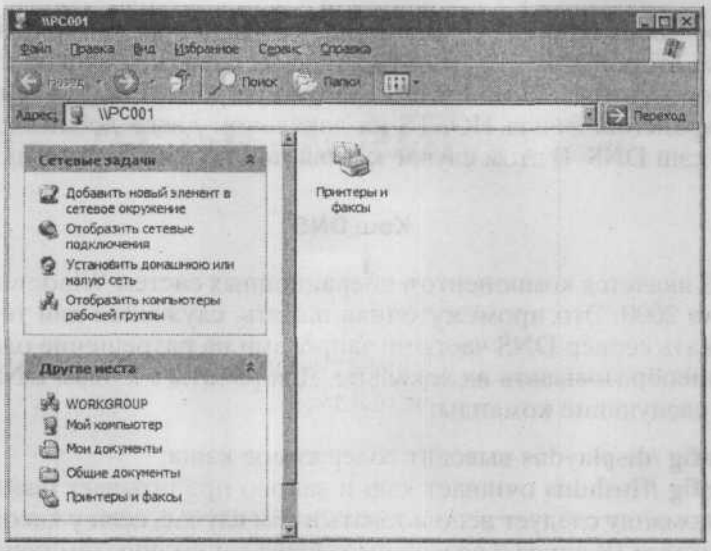


Рис. 6.6. *Разделяемые ресурсы на рабочей станции PC001*

вопрос можно задать и о сервере DNS и файле HOSTS. Знание порядка разрешения имен даст вам возможность в самых сложных сетях выбрать наиболее простое решение, не говоря уже о необходимости этого знания для устранения неполадок с трансляцией имен.

6.5.3. Порядок разрешения имени

Имя узла

Когда вы, сидя за компьютером PC001, отдали команду **ping srvr001**, произошло следующее:

1. Компьютер спросил сам у себя, не является ли SRVR001 его именем. Понятно, что ответ был отрицательным, и поэтому он перешел к следующему шагу.
2. Компьютер открыл свой кэш DNS и проверил, нет ли там записи о том, какому IP-адресу соответствует имя SRVR001. Если его не нашлось, то он перешел к следующему шагу.
3. Компьютер попытался послать запрос на разрешение имени серверу DNS. Нашему компьютеру PC001 посылать запрос некуда, потому что он не знает IP-адреса сервера DNS. На этом преобразование имени узла заканчивается.

На каком же этапе наш PC001 сумел сопоставить имени SRVR001 адрес 192.168.10.2 и какова в этом процессе роль рассмотренного в предыдущем

параграфе файла HOSTS? С ответом на первый вопрос мы пока подождем, а ответ на второй таков. Если файл HOSTS содержит записи с именами узлов и соответствующими им IP-адресами устройств, то эти записи сразу после сохранения файла HOSTS на локальном диске добавляются в локальный кэш DNS. В этом случае компьютер получает ответ на шаге 2.

Кэш DNS

Кэш DNS является компонентом операционных систем Windows, начиная с Windows 2000. Это промежуточная память, служащая для того, чтобы не загружать сервер DNS частыми запросами на разрешение одинаковых имен, а преобразовывать их локально. Для работы с кэшем DNS предназначены следующие команды:

- **ipconfig /displaydns** выводит содержимое кэша;
- **ipconfig /flushdns** очищает кэш и заново прочитывает файл HOSTS. Эту команду следует использовать в том случае, если у какого-то узла изменился IP-адрес и содержимое кэша таким образом перестало соответствовать действительности.

Имя NetBIOS

Когда вы, сидя за сервером SRVR001, вводили команду **Пуск → Выполнить, Открыть** \\PC001, произошло следующее:

1. Компьютер проверил, не является ли \\PC001 UNC-путем к нему самому. Не является, поэтому он перешел к следующему шагу.
2. Компьютер поискал соответствие UNC-пути \\PC001 в своем кэше NetBIOS. Если соответствия не нашлось, он перешел к следующему шагу.
3. Компьютер попытался отправить запрос на разрешение имени PC001 первому из WINS-серверов, IP-адреса которых прописаны в настройках протокола TCP/IP. Если таких адресов не указано или сервер WINS не может найти соответствие запрошенному имени, то компьютер перешел к следующему шагу.
4. Компьютер посылает широковещательный запрос, существует ли в локальной сети такое NetBIOS-имя. Широковещательный запрос не подлежит маршрутизации через выходной шлюз, поэтому, если запрошенного имени в локальной сети нет, а есть оно, например, во внешней сети, то последовал следующий шаг.
5. Последней попыткой найти NetBIOS-имя является просмотр файла LMHOSTS.

Итак, файл LMHOSTS просматривается в последнюю очередь. Но к отдельным записям в этом файле можно дописать ключевое слово #PRE, которое заставляет операционную систему при каждом обновлении кэша

NetBIOS загружать эти записи в кэш, после чего эти имена разрешаются уже на втором шаге.

Файл LMHOSTS всегда анализируется последовательно, поэтому имеет смысл наиболее часто вызываемые имена размещать в его первых строках.

Кэш NetBIOS

Кэш NetBIOS — традиционный компонент Windows, он присутствует и в версиях более ранних, чем Windows 2000. Для работы с ним служат следующие команды:

- **nbtstat -c** — вывод имен удаленных компьютеров из локального кэша (например, здесь отобразятся записи файла LMHOSTS, снабженные ключевым словом #PRE;
- **nbtstat -r** — вывод имен удаленных компьютеров, разрешенных при помощи службы WINS или широковещательного запроса.

А теперь — ответ на вопрос, как же было разрешено имя SRVR001, не найденное в файле HOSTS. В продуктах компании Microsoft поиск имени узла не заканчивается при невозможности обратиться к серверу DNS. Вместо этого операционная система продолжает поиск так, как если бы запрошенное имя было именем NetBIOS, то есть в нашем случае она нашла его по широковещательному запросу в подсети 192.168.10.0/24. Понятно, что если бы запрашиваемое имя было длиннее 15 символов, то применить этот способ было бы невозможно, и его IP-адрес не был бы найден. Если бы сервер SRVR001 находился в другой подсети, то поиск по имени NetBIOS был бы возможен, но дал бы отрицательный результат.

6.6. Зачем использовать службу DNS во внутренней сети

Только что мы рассмотрели случай, когда имя узла успешно разрешается способом, предназначенным для разрешения NetBIOS-имен. Очевидно, что процедура, специально предназначенная для разрешения имен узлов, сработала бы быстрее.

Клиентские компьютеры с Windows 2000 и Windows XP используют в домене с серверной операционной системой Windows Server 2000 или более новой (то есть в домене с Active Directory) исключительно службу DNS. Кроме разрешения имен, сервер DNS выполняет еще одну очень важную роль — обеспечивает информацию о местонахождении служб в сети.

Речь идет о следующем. Чтобы зарегистрироваться на рабочей станции с Windows XP Professional, вы включите компьютер, дождетесь экрана

приветствия, введете свои регистрационные данные (имя и пароль доменной учетной записи). Теперь рабочая станция должна найти контроллер домена, то есть тот компьютер, на котором хранятся доменные учетные записи и который и предоставляет вам доступ к работе. Как, однако, клиент будет его искать? Может быть, адрес контроллера хранится на клиентском компьютере статически?

Нет, это не так. Если бы информация об имени домена хранилась в системе компьютера-клиента, была бы возможна следующая ситуация: вы включаете компьютер после отпуска, а в сети произошли перемены — появился новый контроллер домена, а старый, соответственно, был удален. Естественно, новый контроллер по старым статическим данным найден бы не был и вам не удалось бы зарегистрироваться.

На самом деле клиентские ОС Windows 2000 и Windows XP, работая в домене, обслуживаемом соответствующей им серверной ОС, обращаются за информацией о контроллере домена к службе DNS.

6.7. Установка службы DNS

Службу DNS можно устанавливать только как компонент серверной операционной системы. Ее установка осуществляется по следующему сценарию:

1. Зарегистрируйтесь на сервере SRVR001 как Администратор.
2. Выполните команду **Пуск → Панель управления → Установка и удаление программ**. Выберите действие **Установка компонентов Windows**.
3. В появившемся окне **Мастер компонентов Windows** выберите **Сетевые службы** и нажмите на кнопку **Состав**.
4. В появившемся окне **Сетевые службы** установите флажок **Domain Name Server (DNS)** и нажмите **OK** (рис. 6.8).
5. Нажатием на кнопку **Далее** запустите установку службы DNS. Она не требует перезагрузки системы.

6.8. Настройка службы DNS

Теперь нужно настроить службу DNS. Пространство доменных имен (информация о соответствии имен узлов IP-адресам) организовано иерархически в так называемые зоны. Понятие зоны должно быть уже знакомо вам по работе в Интернете. Иногда вместо слова «зона» говорят «домен», но это не совсем точно: зона может включать пространство нескольких доменов. Далее мы будем использовать исключительно термин «зона».

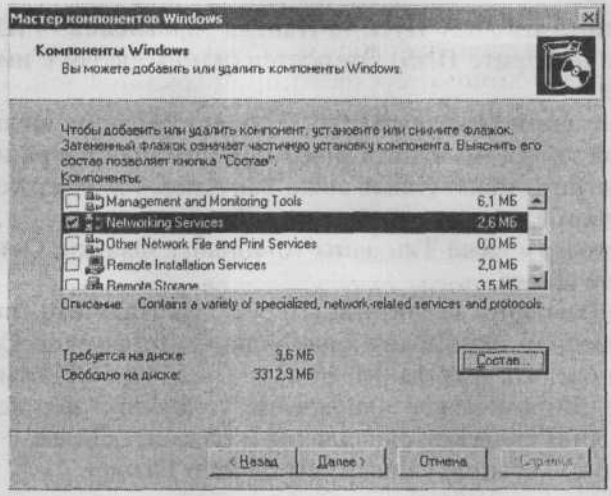


Рис. 6.7. *Установка компонентов Windows*

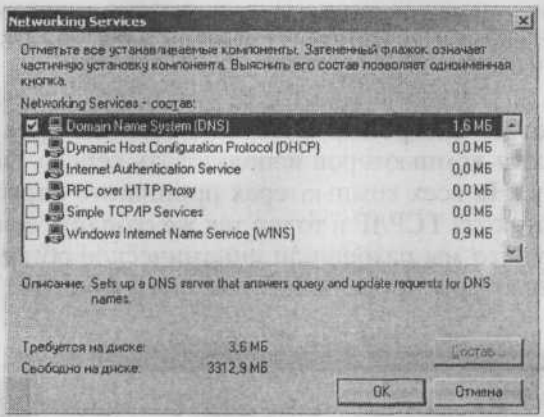


Рис. 6.8. *Установка сетевых служб Windows Server 2003*

Локальная сеть образует одну зону. Нужно выбрать для нее название. Если в ваши намерения не входит «публикация» имен узлов вашей сети в Интернете, то название зоны можете выбирать произвольно. Если же она должна служить для разрешения имен ваших узлов по запросам извне, то нужно получить имя зоны у организации, уполномоченной выдавать доменные имена. Имена второго уровня (уровня страны) выдает национальный координатор, уполномоченный международной организацией InterNIC — в России это RU-CENTER (www.nic.ru), а именами следующих уровней распоряжаются владельцы соответствующих зон.

Поскольку мы создаем зону исключительно для обслуживания локальной сети, назовем ее study.local. Порядок действий по созданию зоны таков:

1. Выполните команду **Пуск → Панель управления → Администрирование** и выберите **DNS**. Откроется окно консоли с именем сервера SRVR001.
2. В левой части окна разверните объект сервера, щелкните правой кнопкой мыши по пункту **Зоны прямого просмотра** и выберите из контекстного меню **Новая зона**. Запустится Мастер создания зоны. На первом шаге нажмите кнопку **Далее**.
3. В диалоговом окне **Тип зоны** установите флажок **Основная зона** и нажмите **Далее**.
4. В поле **Имя зоны** введите `study.local`. Нажмите **Далее**.
5. В диалоговом окне **Файл зоны** установите флажок **Создать новый файл** и введите имя файла: `study.local.dns`. Нажмите **Далее**.
6. В окне **Динамическое обновление** установите флажок **Разрешить любые динамические обновления** и нажмите **Далее**.
7. Завершите установку нажатием кнопки **Готово**.

Примечание.

Пусть вас не смущает предупреждение о небезопасности обновлений данных зоны. Во внутренней сети на него можно не обращать внимания. Более того, в дальнейших главах мы примем дополнительные меры безопасности.

Последним шагом настройки DNS является инструктирование всех имеющихся в сети компьютеров использовать сервер DNS и только что созданную зону. На всех компьютерах пропишите адрес сервера DNS в параметрах протокола TCP/IP и точно так же создайте зону `study.local`. Благодаря тому, что мы разрешили динамическое обновление зоны, все остальное компьютеры проделают без нашего участия.

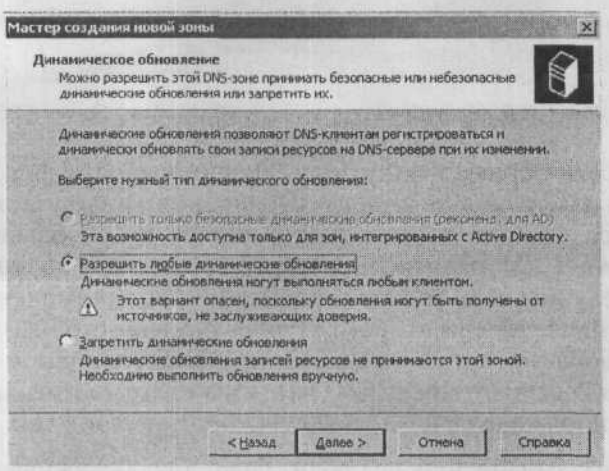


Рис. 6.9. *Разрешение динамических обновлений зоны*

6.8.1. Настройка DNS на сервере SRVR001

Настройка DNS на сервере состоит из следующих шагов:

1. В главном меню выберите **Панель управления → Сетевые подключения**, а затем правой кнопкой мыши щелкните по пункту **Подключение по локальной сети**.
2. Из контекстного меню выберите **Свойства**.
3. В окне свойств подключения к локальной сети выберите пункт **Протокол сети Интернет TCP/IP** и нажмите на кнопку **Свойства**. Откроется окно свойств протокола TCP/IP.
4. В поле **Предпочитаемый сервер DNS** введите IP-адрес сервера SRVR001 — 192.168.10.2. SRVR001 будет сам себе и сервером, и клиентом DNS.
5. Последовательным нажатием на кнопку **OK** закройте все окна.
6. В меню **Пуск** нажмите правой кнопкой мыши на меню **Мой компьютер** и выберите пункт **Свойства**.
7. В диалоговом окне **Свойства системы** откройте вкладку **Имя компьютера** и нажмите кнопку **Изменить**.
8. В диалоговом окне смены имени компьютера нажмите кнопку **Дополнительно**.
9. В диалоговом окне **DNS-суффикс и NetBIOS-имя компьютера** введите в поле **Предпочитаемый DNS-суффикс** имя зоны `study.local`. Нажатием **OK** закройте окно.
10. Вы увидите в диалоговом окне **Смена имени компьютера** в поле **Полное имя компьютера** `srvr001.study.local` — имя, состоящее из имени узла и суффикса DNS. Это имя должно быть уникальным в пределах сети. Диалоговое окно закройте нажатием **OK**.
    После этого необходимо перезагрузить компьютер.
11. После перезагрузки компьютера снова откройте консоль DNS и в левой части окна выберите зону `study.local`. В правой части окна обратите внимание на созданный объект **A (хост)** сервера SRVR001.

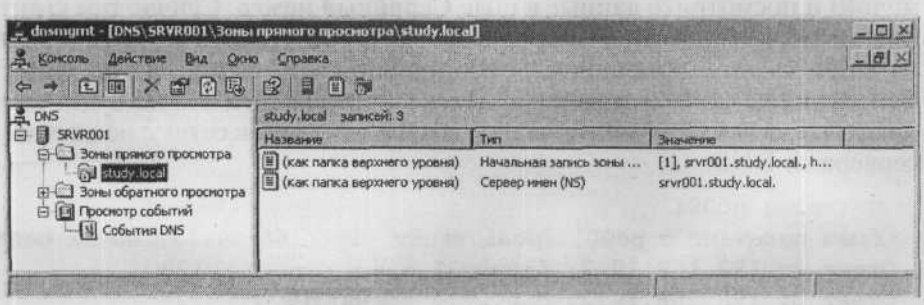


Рис. 6.10. *Вновь созданная зона study.local*

6.8.2. Настройка DNS на рабочей станции

Для настройки DNS на рабочей станции необходимо проделать следующие действия:

1. Зарегистрируйтесь на компьютере PC001 как Администратор.
2. В главном меню выберите **Панель управления → Сетевые подключения**, а затем правой кнопкой мыши щелкните по пункту **Подключение по локальной сети**.
3. Из контекстного меню выберите **Свойства**.
4. В окне **Подключение по локальной сети — свойства** выберите **Протокол сети Интернет**, нажмите на кнопку **Свойства**.
5. В поле **Предпочитаемый DNS-сервер** введите адрес сервера SRVR001 — 192.168.10.2. Затем нажмите **OK**. Диалоговое окно свойств подключения закройте нажатием кнопки **Закрыть**.
6. Далее действуйте так же, как на сервере (пункты с 6 по 10). Для того, чтобы изменения вступили в силу, надо будет перезагрузить компьютер. Закройте оба окна и перезагрузите компьютер.

Перезагрузив компьютер PC001, откройте на сервере SRVR001 окно консоли DNS и отобразите содержание зоны `study.local`. Как видите, здесь появился еще один узел — PC001 с соответствующим ему IP-адресом. Если он пока не отображен, хотя все сделали правильно, подождите еще минуту. Очевидно, в компьютере еще не начали работать сетевые службы.

Примечание.

Система Windows XP Professional устроена так, что она делает возможным вход пользователей еще до активации сетевых служб. Для большинства пользователей это очень важно, потому что регистрация происходит намного быстрее, чем в старых операционных системах. В нашей сети, однако, с этим не все в порядке. Мы вернемся к этой проблеме позже.

В консоли DNS щелкните по записи **Start of Authority (Начало полномочий)** и посмотрите данные в поле **Серийный номер**. Сейчас там стоит 3. Это число, которое имеет первоначальным значением 1 и увеличивается на 1 при каждом изменении. Пока прошло 2 изменения, и оно равно 3. Это число вы можете изменять, однако в нашей сети это не будет иметь никакого эффекта: редактирование его имеет смысл в сетях с несколькими серверами DNS.

```
C:\>ping pc001
Обмен пакетами с pc001.local.study [192.168.10.17] по 32 байт:
Ответ от 192.168.10.2: байты=32 время=2мс TTL=128
Ответ от 192.168.10.2: байты=32 время<1мс TTL=128
```

```
Ответ от 192.168.10.2: байты=32 время<1мс TTL=128
Ответ от 192.168.10.2: байты=32 время<1мс TTL=128
Статистика ping для 192.168.10.17:
Пакетов: отправлено=4, получено=4, потеряно=0 (0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Сравните этот результат с выводом команды **ping pc001** из параграфа 6.5.1. Разница почти незаметна, но очень важна: до настройки службы DNS первая строка вывода выглядела как

```
Обмен пакетами с pc001 [192.168.10.17] по 32 байт:
```

По этой строке вывода можно понять, какая служба сопоставила имени PC001 IP-адрес. Судя по суффиксу `DNS local.study`, во втором случае это была служба DNS, а в первом случае IP-адрес был получен в ответ на широковещательный запрос.

После того, как вы настроите DNS на остальных рабочих станциях точно так же, как вы сделали это для компьютера PC001, можете убедиться, что все эти узлы присутствуют в зоне DNS. Теперь в нашей сети обеспечено правильное, быстрое и точное разрешение имен.

6.9. Итоги

В то время, как пользователи обращаются к другим компьютерам в сети по именам, компьютеры сообщаются друг с другом посредством IP-адресов. IP-адреса очень трудно запоминаемы для пользователей, и поэтому для успешной связи «пользователь-компьютер» нужна служба-посредник.

Каждый компьютер выступает в сети под двумя именами — именем узла и именем интерфейса NetBIOS. Операционные системы начиная с Windows 2000 используют для связи преимущественно имя узла, а более ранние — имя NetBIOS.

Для разрешения имени узла служит статический файл HOSTS или динамическая служба DNS, а для разрешения имен NetBIOS — статический файл LMHOSTS или динамическая служба WINS. Существуют простые способы определить, какая именно служба сработала в каждом конкретном случае.

Служба WINS с самого начала поддерживала динамическое обновление данных. Служба DNS поддерживает динамическое обновление только начиная с Windows 2000 Server. Из клиентских операционных систем только Windows 2000/XP/2003 могут самостоятельно регистрировать имя

своего узла, для более ранних версий это должен делать сервер DHCP — компонент ОС Windows Server 2000/2003.

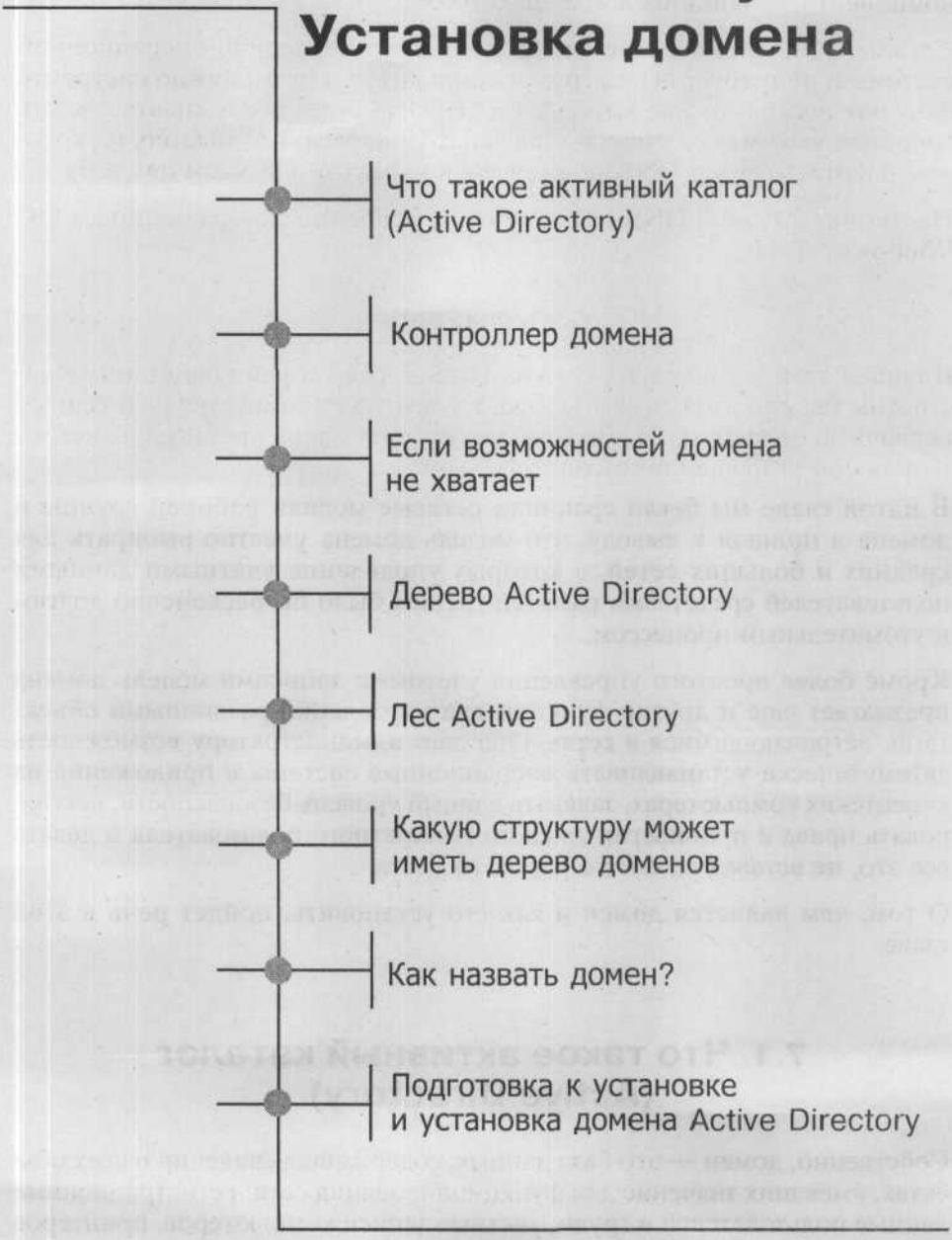
Служба DNS устанавливается как компонент серверной операционной системы и не требует перезагрузки компьютера. Потом нужно настроить одну или несколько зон, которые сервер DNS будет обслуживать, то есть сопоставлять именам узлов в этих зонах IP-адреса. Компьютер, на котором работает сервер DNS, должен быть клиентом DNS сам для себя.

Настройка службы DNS очень проста, особенно по сравнению с ОС Windows NT 4.0.

Состояние сети

В нашей сети установлена служба DNS, сервер и рабочие станции настроены так, чтобы пользоваться ею. У клиентских компьютеров появился первичный суффикс DNS, который указывает, в какой именно зоне искать запись при разрешении имени узла.

Глава 7 Active Directory. Установка домена



В пятой главе мы бегло сравнили сетевые модели рабочей группы и домена и пришли к выводу, что модель домена уместно выбирать для средних и больших сетей, в которых управление учетными данными пользователей средствами рабочей группы было бы бесконечно долгим и утомительным процессом.

Кроме более простого управления учетными записями модель домена предлагает еще и другие функции для управления различными объектами, встречающимися в сетях. Она дает администратору возможность автоматически устанавливать операционные системы и приложения на клиентских компьютерах, задавать единый уровень безопасности, регулировать права и привилегии каждого конкретного пользователя и делать все это, не вставая со своего рабочего места.

О том, чем является домен и как его установить, пойдет речь в этой главе.

7.1. Что такое активный каталог (Active Directory)

Собственно, домен — это база данных, содержащая сведения о всех объектах, имеющих значение для функционирования сети: регистрационные данные пользователей и групп, учетные записи компьютеров, принтеров и других сетевых устройств.

Таким образом, домен можно представить как логическую группу сетевых объектов. Для абсолютного большинства объектов их физическое рас-

положение безразлично, а для некоторых объектов атрибут расположения вообще не имеет смысла.

Домен, или доменная база данных, — это не только собрание объектов (каталог). Эта база данных может также отвечать на вопросы (например, в каком отделе работает пользователь Андрей Васильев), выполняя тем самым роль сервера каталога. В операционной системе Windows Server 2003 так же, как и в Windows 2000 Server, сервер каталога называется Active Directory, или активным каталогом.

Active Directory (AD) — это иерархически организованное хранилище, которое предоставляет удобный доступ к сведениям о различных объектах сети, помогая пользователям и приложениям найти эти объекты. К тому же он проверяет, есть ли у пользователя, запросившего информацию, право на ее получение. Список пользовательских прав также находится в базе данных Active Directory.

7.2. Контроллер домена

Что такое контроллер домена?

Компьютер, на котором работает сервер каталога, называется контроллером домена; иными словами, контроллер домена — это компьютер, на котором размещена вся база данных Active Directory. Все запросы к активному каталогу и вообще все запросы, касающиеся доступа к информации, хранящейся в домене, обрабатывает именно этот компьютер.

Роль управления доменом — настолько важная в сети функция, что от нее напрямую зависит работа сети. Поэтому и доступ к контроллерам домена (DC, Domain Controller) разрешается с большей осторожностью, чем к остальным, а сами эти компьютеры имеют большую степень безопасности (как с точки зрения сетевого доступа, так и чисто физически) и оснащаются самым надежным оборудованием. В крупных сетях они никогда не выполняют дополнительных серверных функций (не бывают серверами печати, приложений, файловыми серверами и т.п.). Реализация доменной модели сети начинается с установки контроллера домена.

Поскольку никакое оборудование не обладает стопроцентной гарантией, может случиться, что через некоторое время контроллер домена выйдет из строя. Что произойдет тогда? Очевидно, что база данных Active Directory перестанет быть доступна, а это значит, что пользователи не смогут зарегистрироваться ни на одном из компьютеров домена. К таким неприятностям нужно готовиться еще на этапе планирования сети, и решением будет организация нескольких контроллеров домена.

Несколько контроллеров домена?

Учетная запись пользователя должна обеспечивать его работу во всем пространстве домена. Если в домене несколько контроллеров, то его учетные записи хранятся на нескольких компьютерах. Не возникнет ли между ними противоречия?

Нет. При установке второго контроллера домена не создается новой базы данных Active Directory, вместо этого на него копируется, или реплицируется, существующая база данных. Таким образом, каждый контроллер домена хранит одни и те же данные, включая учетные записи пользователей. Теперь, если один из контроллеров домена выйдет из строя, клиенты автоматически переключатся на другой, и это нисколько не помешает их работе.

7.3. Если возможностей домена не хватает

Название этого параграфа отнюдь не намекает на то, что существует более эффективная, чем домен, сетевая модель. Такой модели нет. Но к некоторым сетям предъявляются требования, которым не может удовлетворить *один* домен. Дело даже не в том, что максимальное количество объектов в активном каталоге ограничено: в ограничение в несколько миллионов объектов не вписаться трудно. Это ведь не домен операционной системы Windows NT 4.0, в котором могло находиться не более сорока тысяч объектов. Домен Windows Server 2003 можно считать практически безразмерным.

Но обстоятельства, при которых уместной или неизбежной будет организация еще одного домена, существуют. Вот несколько примеров:

- **Административное решение**. Технических причин в этом случае нет, но требование руководства предприятия выполнять нужно.
- **Разные требования к безопасности в разных подразделениях.** Например, если руководство требует, чтобы у пользователей из отдела разработки пароль был не короче 10 символов, а у всех остальных — не короче 8 символов, то эти требования в пределах одного домена выполнить невозможно. Придется выделять разработчиков во второй домен.
- **Разные подразделения должны быть представлены в Интернете под разными именами**. Один домен не может иметь нескольких имен.
- **Перегрузка линий связи**. Когда в домене создается новый объект (например, учетная запись пользователя), то он реплицируется на все контроллеры домена. Если на предприятии два подразделения, связанные между собой медленной и ненадежной линией, то не стоит загружать эту линию еще и копированием содержимого активного

каталога: здесь уместно выделить эти подразделения в отдельные домены.

На практике можно встретить окружение, в распоряжении которого имеется несколько доменов. Речь идет о заграничных отделениях компаний или об очень больших предприятиях. Однако если ваше предприятие не соответствует какой-либо из вышеописанных ситуаций, то вам будет хватать и одного домена.

7.4. Дерево Active Directory

Если в вашей организации несколько доменов, у вас есть две возможности их логической организации. Первая из них называется деревом доменов. Она характеризуется тем, что домены, входящие в дерево, образуют единое пространство имен (рис.7.1). Это значит, что имена объектов должны быть уникальными в пределах всего дерева. Достигается эта уникальность тем, что полное имя подчиненного домена (`europe.microsoft.com`) складывается из его собственного имени (europe) и имени вышестоящего домена (`microsoft.com`). Имя домена высшего уровня (корневого домена) входит в имена всех поддоменов.

На количество доменов, образующих дерево, ограничений нет.

Домены могут быть связаны друг с другом доверительными отношениями. Доверительные отношения означают следующее: пользователь, имеющий учетную запись в домене-доверенном, автоматически получает доступ к разделяемым ресурсам домена-доверителя. Отношение доверия транзитивно: если домен A доверяет домену B, а домен B доверяет домену C, то домен A доверяет домену C.

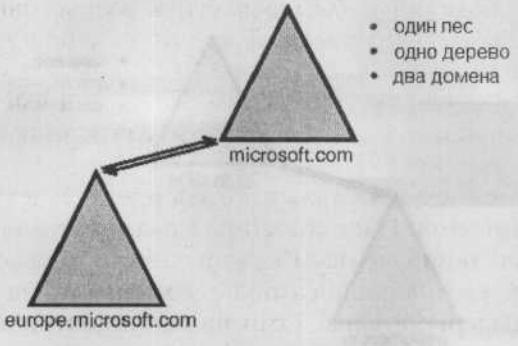


Рис. 7.1. *Пример дерева Active Directory*

При создании нескольких доменов в одном дереве Active Directory автоматически устанавливаются междоменные двунаправленные доверительные отношения.

Новый домен, организуемый в рамках дерева, автоматически вступает в доверительные отношения со старыми, причем эти отношения двунаправленные: если домен A доверяет домену B, то домен B доверяет домену A. Таким образом, пользователь может, зарегистрировавшись только в одном домене, получить доступ ко всем ресурсам всех доменов дерева.

7.5. Лес Active Directory

Другая модель логической организации доменов — лес.

Начнем с примера. Пусть компания Study, имеющая свой домен `study.local`, приобрела компанию Instrument, также имеющую свой домен `instrument.ru`. В ходе слияния фирм требуется объединить два имеющихся домена в одну структуру для удобства управления ими, но имена всех сетевых объектов желательно сохранить: этого требуют, например, используемые в компаниях приложения. Сохранить имена, объединив домены в дерево, невозможно: у них нет общего корня. Решением будет создание леса, то есть набора из одного или нескольких деревьев, не образующих единого пространства имен.

Все деревья леса связаны двусторонними транзитивными доверительными отношениями.

Главное различие между деревом доменов и лесом заключается в том, что все домены, входящие в дерево, должны иметь общий корневой домен, а для доменов, образующих лес, это необязательно. Нужно добавить, что подобно тому, как количество доменов в дереве не ограничено, не ограничено и количество деревьев в лесу.

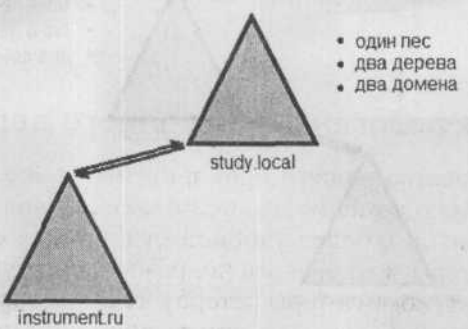


Рис. 7.2. *Лес Active Directory с двумя деревьями*

7.6. Какую структуру может иметь дерево доменов

Если вы устанавливаете единственный домен, то для создания дерева ничего дополнительно организовывать не нужно: корневым доменом дерева Active Directory становится тот домен, который вы устанавливаете первым. Получается лес из одного дерева, содержащего один домен. Интереснее ситуация, когда предприятию требуется несколько доменов.

7.6.1. Добавление домена к существующему дереву

Допустим, вам нужно установить сеть в московском филиале петербургского предприятия. На головном предприятии уже существует домен Active Directory, и новый домен должен либо быть подчинен ему, либо стать корнем нового дерева. Второе решение неоправданно, поскольку во вновь устанавливаемом домене еще нет сетевых имен, которые требовалось бы сохранить. Поэтому выбирайте первое решение, в результате которого сеть получит структуру, приведенную на рис. 7.3.

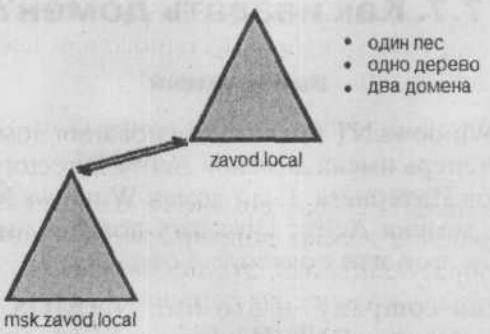


Рис. 7.3. Дерево с добавленным доменом

7.6.2. Организация нового дерева

Допустим, руководство нашего предприятия заранее знает, что ему понадобится несколько доменов для нескольких филиалов. С точки зрения управления, возможно, более удобной будет такая структура сети, при которой компьютеры московского подразделения будут членами домена `msk.zavod.local`, компьютеры петербургского подразделения — членами домена `spb.zavod.local`, а при расширении предприятия домены новых филиалов подключались бы на том же самом уровне.

Рис. 7.4. *Вновь организованное дерево*

Тогда понадобится еще один домен, который будет служить корневым для доменов подразделений — `zavod.local`. Структура сети будет выглядеть так, как на рис. 7.4.

7.7. Как назвать домен?

Выбор имени

По сравнению с Windows NT правила именования доменов Active Directory изменились: теперь имена доменов Active Directory выглядят так же, как имена доменов Интернета. Если домен Windows NT мог называться company, то имя домена Active Directory должно иметь хотя бы один суффикс: `company.com` или `company.local`.

Само по себе имя company — это имя NetBIOS, в то время, как `company.com` — это имя DNS. Начиная с Windows 2000, имена DNS стали основным средством именования узлов сети; более ранние версии ОС Windows пользуются преимущественно NetBIOS-именами. В целях обратной совместимости нужно было узаконить оба варианта имени домена, и в Active Directory так и сделано: клиентским компьютерам под управлением Windows NT 4.0 Workstation домен будет известен как company, а клиентам под управлением Windows XP Professional — под именем company.com.

Если вы решили устанавливать домен Active Directory в системе Windows 2000 Server, нужно прежде всего тщательно выбрать для него имя, ведь потом его невозможно будет поменять. Имя корневого домена служит «электронной визитной карточкой» предприятия. Оно входит составной частью в имена других доменов того же дерева. При его выборе необхо-

димо учитывать задачи предприятия, известность имени пользователям, представленность его в Интернете и способ управления зоной DNS Интернет-домена

Какой суффикс выбрать для имени домена?

Как уже сказано, суффикс является необходимой составной частью имени домена. Поскольку домены Active Directory именуются так же, как домены Интернета, то возникают две возможности:

- **Суффикс, совпадающий с именем Интернет-домена верхнего уровня** (com, org, ru, ua). Если у предприятия уже есть зарегистрированное доменное имя company.com, то оно может использовать суффикс com и для домена Active Directory. Если предприятие пока в Интернете не представлено, то впоследствии оно сможет использовать для представительства готовое имя домена AD — при условии, что не возникнет конфликта с чужим ранее зарегистрированным доменным именем.
- **Суффикс, который нельзя использовать в Интернете**. Если предприятие не собирается регистрировать свой домен AD как Интернет-домен, то в качестве суффикса можно использовать что угодно, например, `local`.

У каждого варианта есть свои плюсы и минусы. Все зависит от того, что в конкретном случае будет выгодно предприятию. Обычно администраторы руководствуются правилом: если предприятие имеет или планирует завести Интернет-представительство (`company.com`), то имя внутреннего домена должно быть другим, таким, которое невозможно использовать в Интернете (`company.local`). Дело в том, что предприятие само управляет зоной DNS своего Интернет-домена, и такое решение позволяет отделить управление этой зоной от управления зоной DNS для нужд домена Active Directory.

Поскольку наше учебное предприятие Study определенно намерено впоследствии выйти в Интернет, для его внутренней сети мы и выбрали суффикс `local`.

Если мы будем устанавливать домен в системе Windows 2000 Server, нужно отнестись к выбору имени очень внимательно, поскольку потом изменить его будет невозможно. В Windows Server 2003 же имя домена Active Directory изменить можно. Для этого служит утилита **Domain Rename Tool**, которая находится на установочном компакт-диске; ее также можно скачать с сайта компании Microsoft.

7.8. Подготовка к установке домена

Подготавливаем необходимые сведения для установки домена

В этой главе мы установим корневой домен Active Directory. К его установке нужно подготовиться так же тщательно, как и к любой другой установке, собрав всю необходимую информацию.

- **Операционная система**. Функцию контроллера домена может выполнять любой компьютер с серверной операционной системой — в нашем случае это любая система из семейства Windows Server 2003.
- **Необходимые полномочия**. Для установки первичного контроллера домена нужно зарегистрироваться на нем как локальный Администратор.
- **Имя домена DNS**. Именам доменов посвящен предыдущий параграф. Для нашего домена мы выбрали имя DNS study.local.
- **NetBIOS-имя домена**. Это имя предназначено для клиентских операционных систем более ранних версий, чем Windows 2000, которые используют преимущественно NetBIOS-имена. Установочная программа по умолчанию предлагает в качестве NetBIOS-имени первую часть имени DNS (в нашем случае study) — мы рекомендуем согласиться.
- **Размещение важных файлов домена**. В ходе установки нужно будет указать, где будет храниться база данных Active Directory, журнал транзакций и папка SYSVOL. Базу данных и журнал транзакций всегда можно переместить, папку же SYSVOL — никогда.
- **Совместимость с ранними версиями Windows**. Если серверами сети будут только компьютеры под управлением Windows 2000 Server или ОС семейства Windows Server 2003, заботиться о совместимости не нужно. Клиентских компьютеров эта рекомендация не касается.
- **Пароль для восстановления службы каталогов**. Если в будущем вам понадобится восстановить домен Active Directory, загрузите контроллер домена в режиме обновления и зарегистрируйтесь на нем как администратор, введя пароль, заданный при установке домена.
- **Сетевые компоненты.** Сервер, который возьмет на себя управление доменом, должен иметь правильно сконфигурированные сетевые протоколы, и его сетевое подключение должно быть активно (сетевой адаптер должен быть присоединен к сети).

Служба DNS

Сервер каталогов Active Directory тесно связан со службой DNS. Собственно говоря, без нее он работать не будет. Он использует эту службу для поиска информации в сети точно так же, как и клиентские компьютеры. Сервер DNS — еще один важный компонент для правильного функционирования домена Active Directory.

В нашей сети мы уже установили сервер DNS и создали зону DNS под именем, соответствующим задуманному имени домена Active Directory `study.local`. Исходя из того, что служба DNS — неотделимая составная часть домена Active Directory, мастер установки домена производит ее поиск и, если она еще не установлен, предлагает ее автоматическую установку и настройку.

Согласиться с этим можно тогда, когда компьютер, на который устанавливается контроллер управления доменом, одновременно будет служить и сервером DNS. Если же в сети несколько серверов, то рекомендуется освободить контроллер домена от других серверных служб. В этом случае сервер DNS должен быть установлен и настроен заранее.

7.9. Установка домена Active Directory

7.9.1. Последовательность действий при установке

Для установки домена Active Directory выполните следующую последовательность действий:

1. Зарегистрируйтесь на сервере **SRVR001** как Администратор. В командной строке (**Пуск → Выполнить,** в поле **Открыть** введя cmd) введите команду **dcpromo**. Она запустит **Мастер установки службы Active Directory**. Нажмите кнопку **Далее**.
2. Прочитайте сведения, приведенные в диалоговом окне **Совместимость с операционными системами,** и нажмите кнопку **Далее**.
3. В диалоговом окне **Тип контроллера домена** оставьте переключатель в положении **Контроллер домена в новом домене** и нажмите кнопку **Далее.**
4. В диалоговом окне **Создать новый домен** оставьте переключатель в положении **Новый домен в новом лесу** и нажмите кнопку **Далее**.
5. В диалоговом окне **Новое имя домена** введите в поле **Полное DNS-имя нового домена** `study.local` и нажмите кнопку **Далее**.
6. В диалоговом окне **NetBIOS-имя домена** оставьте имя по умолчанию STUDY и продолжите нажатием кнопки **Далее**.
7. В диалоговом окне **Папки базы данных и журналов** оставьте предложенный путь C:\WINDOWS\NTDS для базы данных и C:\WINDOWS\NTDS для журнала. Затем нажмите **Далее**.

Примечание.

С точки зрения оптимизации работы контроллера домена выгоднее было бы поместить файлы базы данных и журнала на разные физические диски, но мы считаем, что у нас всего один жесткий диск.

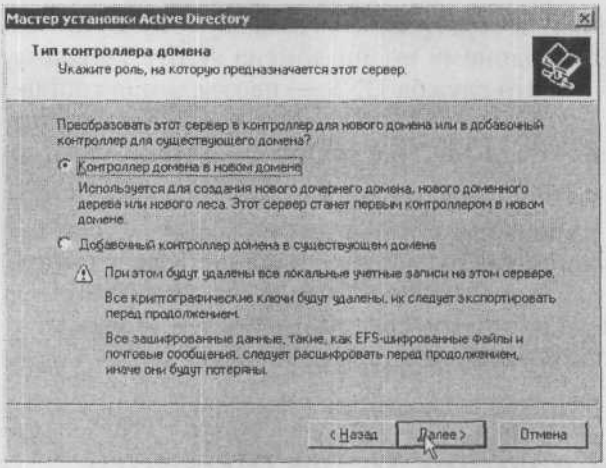


Рис. 7.5. *Создание нового домена Active Directory*

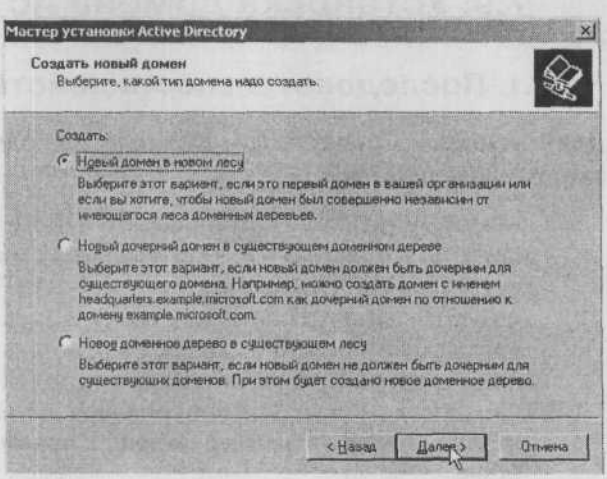


Рис. 7.6. *Создание нового леса Active Directory*

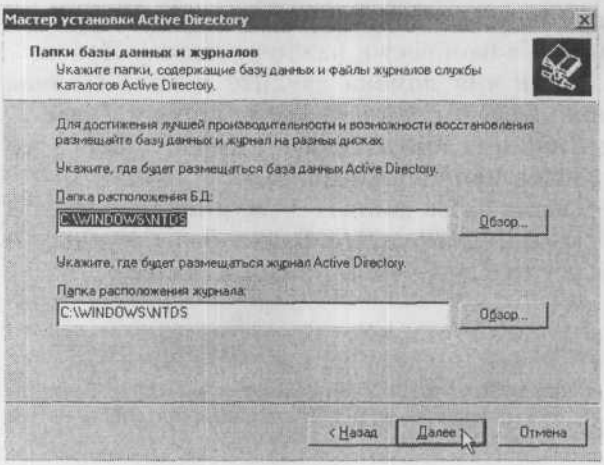


Рис. 7.7. *Размещение базы данных домена Active Directory и журнала транзакций*

8. В диалоговом окне **Общий доступ к системному тому** оставьте предложенный путь C:\WINDOWS\SYSVOL и нажмите **Далее**.

Примечание.

Папку SYSVOL нельзя переместить в дальнейшем. Необходимо, однако, обеспечить, чтобы на диске, на который должна быть осуществлена установка, было достаточно места. Как мы потом увидим, эта папка содержит объекты групповых политик, из-за которых она занимает много места, и если на диске места недостаточно, то это вызовет проблемы с функциональностью домена.

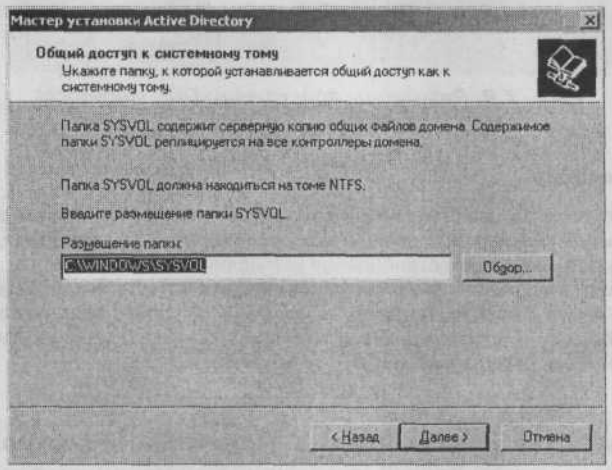


Рис. 7.8. *Размещение системного тома SYSVOL*

9. Теперь сервер произведет поиск зоны DNS по имени, соответствующему заданному имени домена. Если зона будет найдена, отобразится уведомление об успешно проведенной диагностике. Если нет — система предложит ее автоматическую установку и конфигурирование. Прочитав информацию, нажмите кнопку **Далее**.
10. В диалоговом окне **Разрешения** отметьте пункт **Разрешения, совместимые только с Windows 2000** или **Server Windows Server 2003**, а затем нажмите кнопку **Далее**.
11. В диалоговом окне **Пароль администратора для режима восстановления** задайте в поле **Пароль режима восстановления** и в поле **Подтверждение пароля** пароль, который вы используете при восстановлении базы данных Active Directory. Затем нажмите кнопку **Далее**.

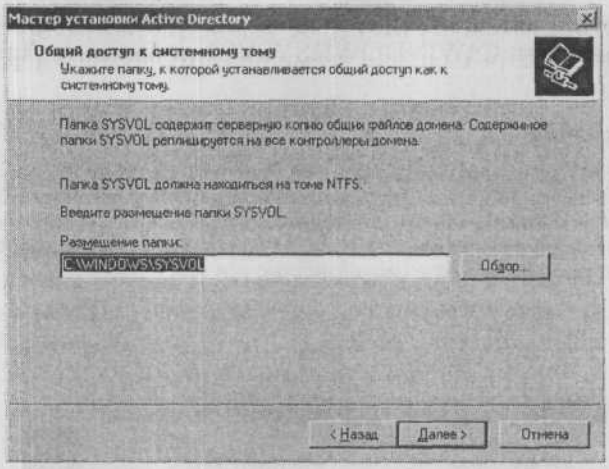


Рис. 7.9. *Результаты поиска зоны DNS study.local*

Примечание.

Не используйте в качестве пароля восстановления обычный пароль администратора. Пароль администратора домена должен периодически меняться, в то время как пароль для режима восстановления всегда остается неизменным. На практике вы можете столкнуться с тем, что после двух лет работы нужно будет восстановить домен Active Directory, но никто не вспомнит пароль, предназначенный именно для этого случая. Поэтому хорошо было бы записать этот пароль и поместить в какое-нибудь безопасное место.

Если вы будете устанавливать дополнительный контроллер домена, выберите для него другой пароль восстановления и тоже где-нибудь запишите.

12. В диалоговом окне **Итоговый результат** проверьте исправность настройки всех параметров домена Active Directory. В случае выявления каких-либо ошибок нажатием на кнопку **Назад** вернитесь к диалоговому окну и исправьте необходимые параметры. Потом нажатием кнопки **Далее** запустите дальнейший процесс установки контроллера домена.
13. По окончании работы Мастера установки службы Active Directory нужно перезагрузить компьютер.

7.9.2. Проверка правильности установки контроллера домена

Сервер SRVR001 сейчас также управляет и доменом Active Directory `study.local`. После установки каждого контроллера домена следует провести контроль качества установки:

1. Зарегистрируйтесь на SRVR001 как Администратор (только администратор теперь обладает всеми правами доступа в домене `study.local`).
2. Запустите Проводник и убедитесь, что существует папка C:\WINDOWS\NTDS с файлами NTDS.DIT (база данных Active Directory) и EDB.LOG (файл журнала транзакций). Далее убедитесь в существовании папки C:\WINDOWS\SYSVOL.
3. В меню **Пуск** перейдите в раздел **Администрирование** и убедитесь, что там добавились инструменты для управления доменом: консоли **Active Directory — пользователи и компьютеры**, **Active Directory — сети и сервисы** и **Active Directory — домены и доверие**. Затем откройте окно консоли **Просмотр событий** и убедитесь, что там добавились пункты **Служба каталогов** и **Служба репликации файлов**. Выберите пункт **Служба репликации файлов** и найдите событие 13516. Там сообщается, что контроллер домена выполняет свои функции (см. рис. 7.10).
4. Откройте консоль **DNS** и убедитесь, что в зоне `study.local` были созданы поддомены `_msdcs`, `_sites`, `_tcp`, `_udp`, `DomainDnsZones` и `ForestDnsZones`. Первые четыре поддомена очень важны для функционирования домена Active Directory. Они включают в себя т.н. списки SRV (Размещение сервиса — Service location), на основании которых все компьютеры с системами Windows 2000/XP/2003 ориентируются в сети при поиске важных сервисов.

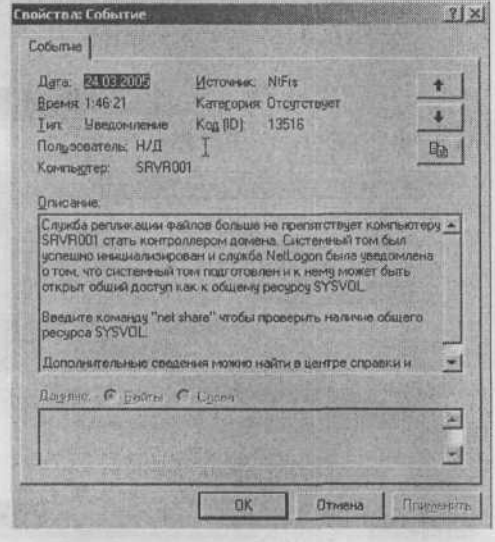


Рис. 7.10. *Событие 13516 в журнале службы репликации файлов*

5. В командной строке введите команду **net share**. Отобразятся разделяемые папки компьютера, в том числе и папка с сетевым именем NETLOGON, которое сопоставлено папке C:\WINDOWS\SYSVOL\study.local\SCRIPTS.

Примечание.

Папка NETLOGON имеет большое значение для ОС версий предшествующих Windows 2000. Она содержит, например, сценарии, запускаемые при регистрации пользователя. В системах Windows 2000/XP/2003 сценарии входа используются несколько иным способом и размещены в другой папке.

7.9.3. Настройка службы DNS на контроллере домена

Сервис DNS сейчас включает только зону `study.local`. Это первичная зона, в которой разрешено динамическое обновление (рис. 7.11).

Разрешение динамического обновления — не вполне безопасная с точки зрения защиты сети вещь. Теоретически может случиться, что некий пользователь переименует свой компьютер в SRVR001 и перезагрузит его. При динамическом обновлении зоны запись, соответствующая имени SRVR001, будет переписана, сопоставив этому имени IP-адрес клиент-

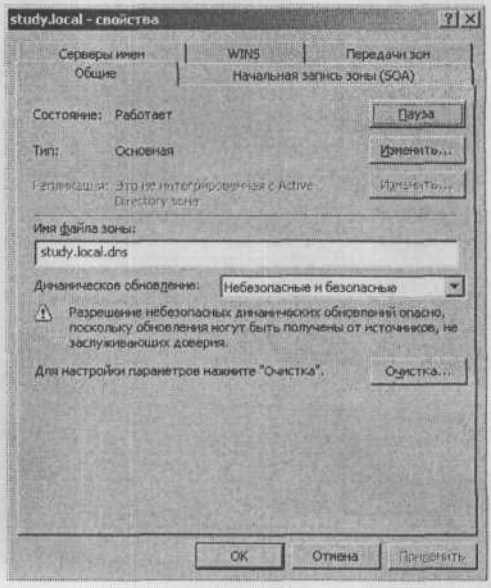


Рис. 7.11. *Свойства зоны study.local*

ского компьютера. После этого все запросы, адресованные серверу, будет получать этот клиент и домен перестанет функционировать.

Нужно так обезопасить зону, чтобы подобная ситуация была полностью исключена или по крайней мере максимально снизить ее вероятность.

До сих пор вы выполняли все административные действия как локальный Администратор, но здесь самое время сказать, что управлять сервером DNS может и обычный пользователь, если он является членом группы DnsAdmins. Возможность распределить администраторскую нагрузку полезна в крупных сетях с децентрализованным управлением.

1. Зарегистрируйтесь на SRVR001 и откройте консоль DNS.
2. Разверните дерево **Зоны прямого просмотра**, правой кнопкой мыши щелкните по зоне `study.local` и из контекстного меню выберите пункт **Свойства.**
3. На вкладке **Общие** нажмите кнопку **Изменить,** а затем установите флажок **На все DNS-серверы в лесу study.local Active Directory** (он доступен только если сервер DNS также управляет доменом). Нажмите кнопку **OK** и в следующем диалоговом окне — кнопку **Да.**
4. Из списка **Динамические обновления** выберите **Только безопасные** и нажмите **OK**.
5. Запустите Проводник и убедитесь, что в папке C:\WINDOWS\SYSTEM32\DNS не существует файла study.local.dns. Информация файла study.local.dns после изменения типа зоны стала составной частью базы данных домена Active Directory, а файл был перемещен в папку BACKUP.

7.9.4. Настройка клиентских компьютеров

Последовательность настройки

Все рабочие станции нужно включить во вновь созданный домен. Действуйте согласно следующим инструкциям:

1. Зарегистрируйтесь на PC001 как Администратор.
2. В меню **Пуск** правой кнопкой мыши щелкните по пункту **Мой компьютер** и из контекстного меню выберите **Свойства.**
3. На вкладке **Имя компьютера** нажмите кнопку **Изменить**. Установите переключатель **Является членом** в положение **домена** и введите имя study.local. Затем нажмите кнопку **OK**.
4. В диалоговом окне изменения имени компьютера задайте имя **Administrator** и пароль и нажмите на кнопку **OK**. В домене будет создана учетная запись компьютера PC001, а на экране отобразится окно с надписью **Добро пожаловать в домен study.local**.

5. Последовательным нажатием на все кнопки **OK** и **Да** проведите перезагрузку компьютера.

Если учетную запись компьютера в домене создать не удалось, то проблема, скорее всего, в неправильной настройке службы DNS. Попытайтесь исправить настройку следующим образом:

1. В главном меню щелкните правой кнопкой мыши по пункту **Мой компьютер** и из контекстного меню выберите **Свойства**. На вкладке **Имя компьютера** в поле **Полное имя** должно отобразиться имя `pc001.study.local`. Если суффикса `study.local` нет, то откройте диалог DNS-суффикса нажатием кнопок **Изменить** и **Дополнительно.** Впишите этот суффикс в поле **Основной DNS-суффикс этого компьютера** и перезагрузитесь.
2. После перезагрузки выберите в главном меню **Панель управления → Сетевые подключения,** затем правой кнопкой мыши щелкните по иконке **Подключение по локальной сети** и из контекстного меню выберите пункт **Свойства**.
3. Выберите **Протокол сети Интернет (TCP/IP)** и нажмите кнопку **Свойства**.
4. В разделе свойств протокола **TCP/IP** нажмите на кнопку **Дополнительно**, а затем перейдите на вкладку **DNS**. Проверьте, правильно ли задан IP-адрес сервера DNS (192.168.10.2) и установлен ли флажок **Дописывать родительские суффиксы осн. DNS-суффикса** (рис. 7.12).

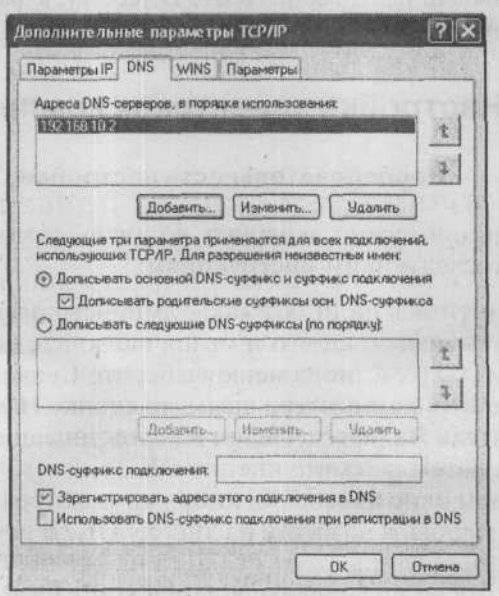


Рис. 7.12. *Правильная настройка параметров DNS*

Если нет, то поставьте. Закройте диалоговое окно последовательным нажатием кнопок **OK**.

5. Запустите режим командной строки и введите команду **ping study.local.** Если вы получили ответ, значит, подключение к сети и передача пакетов в порядке, а служба DNS работает нормально.
6. Если даже после этого компьютер не подключается к домену, убедитесь в нормальной работе контроллера домена, проверьте в том числе настройку протокола TCP/IP так, как это описано в третьей главе.

Проверка присутствия учетной записи компьютера в домене

Данная проверка осуществляется следующим образом:

1. Зарегистрируйтесь на SRVR001 как Администратор.
2. В меню **Пуск** выберите **Администрирование → Active Directory — пользователи и компьютеры**.
3. В левой части открывшегося окна щелкните по контейнеру **Компьютеры**. В правой части появится список учетных записей имеющихся компьютеров.
4. В левой части окна щелкните по контейнеру **Контроллеры домена**, а в правой части проверьте наличие учетной записи управляющего доменом компьютера SRVR001.

Примечание.

В целях безопасности учетные записи контроллеров домена в базе данных Active Directory собраны в отдельную организационную единицу. Не перемещайте их оттуда.

7.9.5. Настройка регистрации пользователей

Операционные системы Windows XP и серверное семейство Windows Server 2003 запускаются быстрее, чем их предшественники Windows Server 2000. Дело не в том, что изменилось ядро системы, вследствие чего она стала быстрее загружаться. Просто по умолчанию система выводит окно регистрации пользователя, не дожидаясь запуска сетевых служб. Для владельцев домашних компьютеров, не подключенных к локальной сети, это удобно, но в домене передача регистрационных данных пользователя из-за этого замедляется. Отключить этот режим (что рекомендуется) можно следующим образом:

1. Зарегистрируйтесь на SRVR001 как Администратор.
2. В меню **Пуск** выберите **Администрирование → Active Directory — пользователи и компьютеры**.

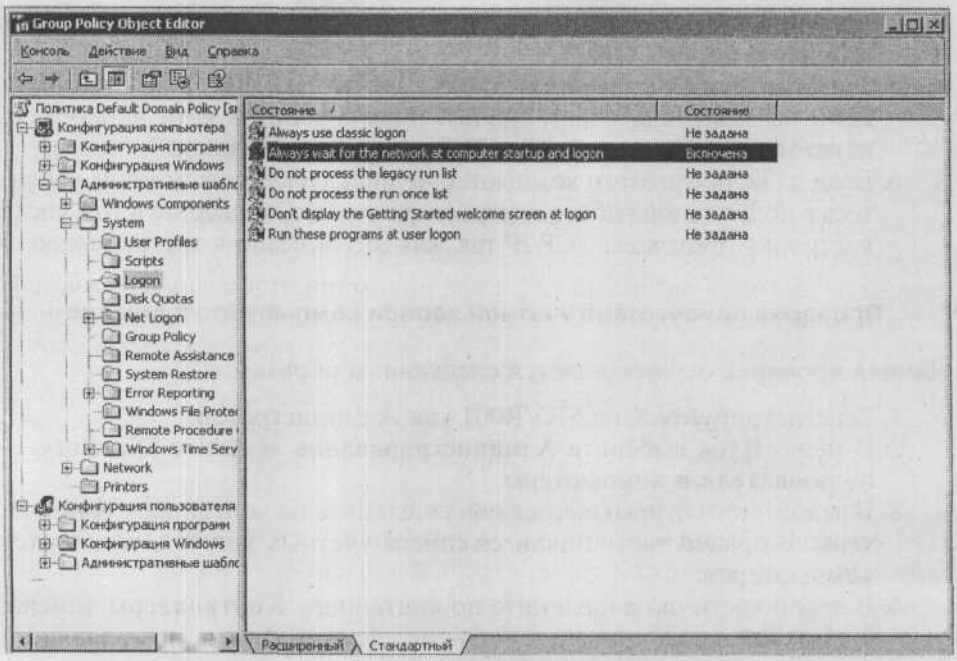


Рис. 7.13. *Настройка политики входа в домен*

3. Правой кнопкой мыши щелкните по домену `study.local` и из контекстного меню выберите **Свойства**. Отобразится диалоговое окно свойств домена.
4. На вкладке **Групповая политика** нажмите **Default Domain Policy**. Откроется окно консоли редактора групповых политик.
5. В левой части окна консоли разверните ветвь **Конфигурация компьютера** → **Административные шаблоны** → **Система** и выберите пункт **Logon (Вход)**.
6. В правой части окна включите режим **Always wait for the network at computer startup and logon (При включении компьютера и входе пользователя всегда дожидаться ответа сети)** и нажмите кнопку **OK**.

7.10. Итоги

Домен Active Directory по сравнению с его предшественником, доменом SAM системы Windows NT 4.0 Server, обладает многими преимуществами. Он может хранить сведения о значительно большем количестве сетевых объектов (учётные записи пользователей, учётные записи компьютеров, группы и т.д.), позволяет делегировать администраторские полномочия с целью облегчить управление крупной сетью либо повысить ее безопасность.

Иногда для организации локальной сети предприятия одного домена не хватает. Чаще всего это касается предприятий с несколькими филиалами или недавно слившихся компаний. В их доменной структуре может присутствовать несколько доменов, организованных по модели дерева или леса Active Directory.

Дерево Active Directory содержит один или несколько доменов, образующих единое пространство имен. Имена доменов в дереве организованы иерархически, а управление ими — нет: администратор вышестоящего домена не получает автоматически прав на администрирование нижестоящего. Единственным привилегированным доменом является тот, который был установлен первым, все остальные домены в дереве равноправны.

При слиянии двух компаний, имеющих домены, может понадобиться сохранить их имена. В этом случае для общей сети следует применить модель леса, в котором два имеющихся домена образуют два независимых дерева.

При установке корневого домена следует тщательно продумать его имя, потому что оно войдет составной частью в имена всех нижестоящих доменов.

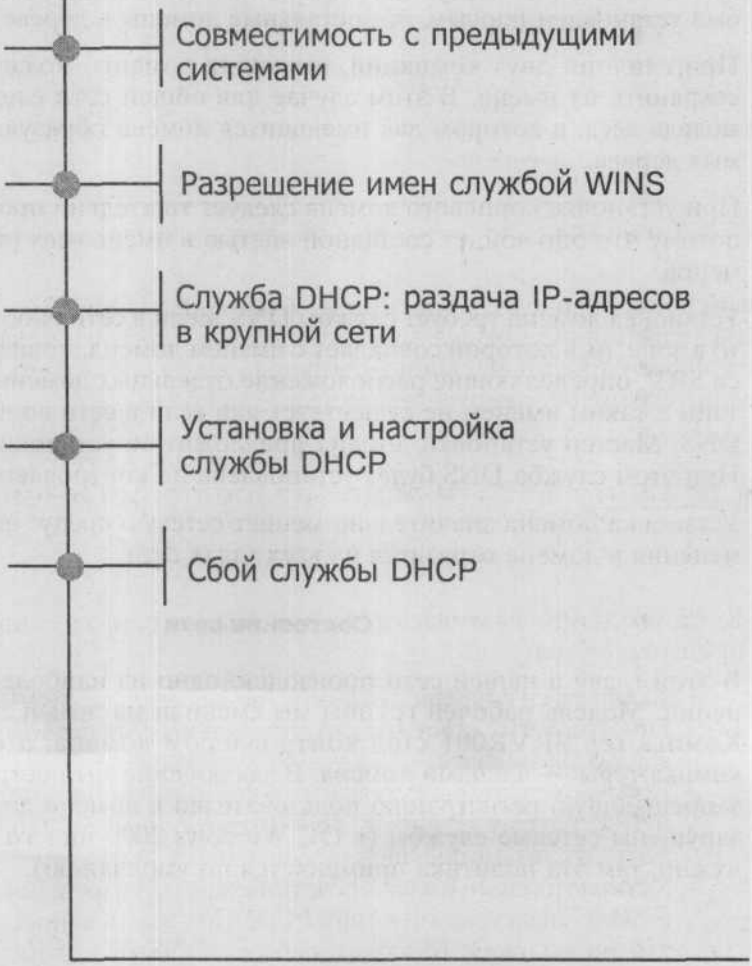
Установка домена требует службы DNS. Если в сети работает эта служба, то в зоне, имя которой совпадает с именем домена, появятся новые записи SRV, определяющие расположение отдельных доменных служб. Если зоны с таким именем не существует или если в сети вообще нет службы DNS, Мастер установки домена предложит ее установить и настроить. При этом служба DNS будет установлена на контроллере домена.

Установка домена значительно меняет сетевую среду: последующие изменения в домене отразятся на всех узлах сети.

Состояние сети

В этой главе в нашей сети произошло одно из наиболее важных изменений. Модель рабочей группы мы сменили на домен Active Directory. Компьютер SRVR001 стал контроллером домена, а все клиентские компьютеры — членами домена. В заключение мы настроили политику, запрещающую регистрацию пользователей в домене до того, как будут запущены сетевые службы (в ОС Windows 2000 ничего настраивать не нужно, там эта политика применяется по умолчанию).

Глава 8 Другие сетевые службы (WINS и DHCP)



Каждый разумный администратор сети стремится как можно более эффективно выполнять свою работу, то есть решать как можно больше задач, затрачивая как можно меньше усилий. Логично было бы предположить, что чем однороднее система, которой вы управляете, тем меньше у вас работы. Примером из уже рассмотренной области является разрешение имен объектов сети.

В то время как системы Windows 2000 Professional и более поздние обращаются к сетевым устройствам по именам узлов и для разрешения этих имен в IP-адреса используют службу DNS, более ранние версии Windows (например, Windows 9x, NT 4.0) работают с NetBIOS-именами и разрешают их посредством других служб. Смешанные системы, то есть системы, в которых функционируют и Windows 2000-2003, и ОС предшествующих версий, встречаются довольно часто, поэтому администратор обязан уметь настраивать соответствующие службы.

Другой пример — IP-адресация сетевых устройств. Когда их количество в вашей сети превысит некоторый уровень, удобно будет назначать устройствам IP-адреса не вручную, а автоматически при помощи определенной сетевой службы.

В этой главе мы рассмотрим настройку службы WINS, предназначенной для разрешения NetBIOS-имен, и службы DHCP, автоматически раздающей адреса и настраивающей протокол IP для различных сетевых устройств (компьютеров, принтеров и т.п.).

8.1. Совместимость с предыдущими системами

Поскольку мы уже установили службу DNS и домен Active Directory, мы можем на конкретном примере показать различия между системами Windows XP Professional и Windows NT 4.0 Workstation.

В 6 главе мы упомянули о процессе поиска контроллера домена Active Directory. Рассмотрим этот процесс немного подробнее, благодаря чему использование домена Active Directory станет понятнее.

8.1.1. Компьютер под управлением Windows XP Professional

Для регистрации пользователя в домене операционная система Windows XP Professional обращается к службе DNS следующим образом:

1. После того как пользователь введет свои регистрационные данные, вызывается служба регистрации в сети (Netlogon), которой клиентский компьютер передает все параметры, необходимые при поиске контроллеров домена: собственный IP-адрес, первичный суффикс DNS и другие.
2. Служба Netlogon, в свою очередь, запрашивает у службы DNS запись типа SRV в формате `_ldap._tcp.dc_msdcs.название_домена`, в нашем случае на `_ldap._tcp.dc._msdcs.study.local` (рис. 8.1).
3. На рис. 8.1 в поле **Узел этой службы** указан компьютер srv001.study.local — это DNS-имя контроллера домена. Чтобы клиент мог обратиться к нему по IP-адресу, служба Netlogon должна послать следующий запрос — разыскать соответствующую запись типа A (рис. 8.2).

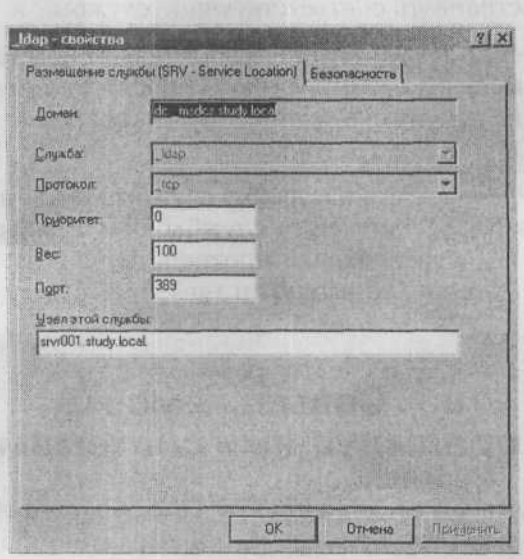


Рис. 8.1. *Запись типа SRV в зоне study.local*

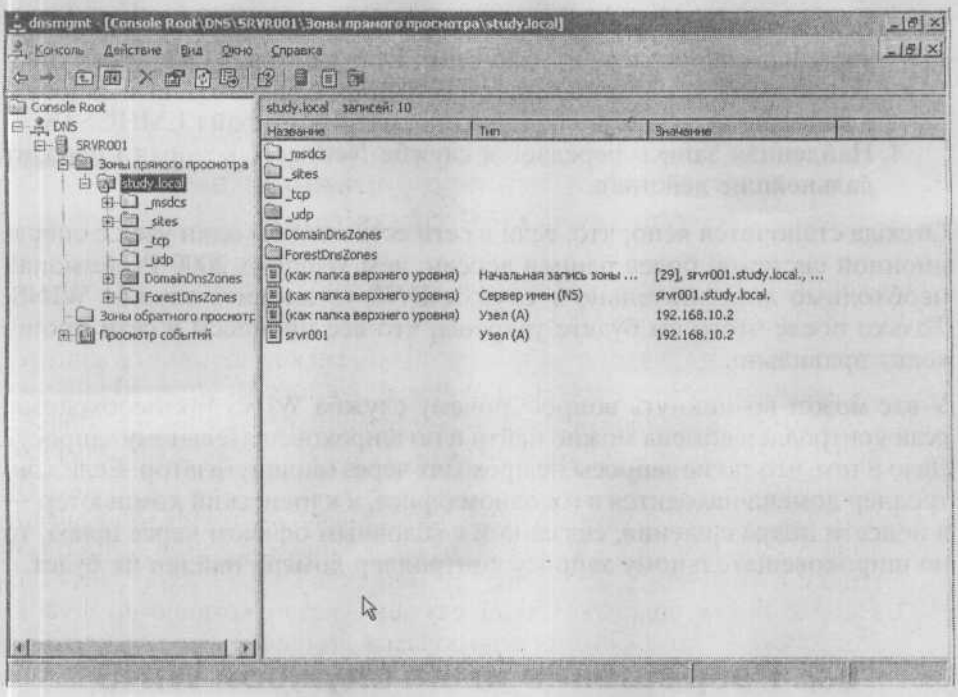


Рис. 8.2. *Запись типа A в зоне study.local*

4. После этого клиентский компьютер обращается к контроллеру домена по полученному IP-адресу и получает таким образом доступ к базе данных Active Directory, где и проверяет регистрационные данные пользователя.

Приведенный процесс максимально упрощен для наилучшего понимания. Снова стоит повторить, что надежность работы домена зависит кроме всего прочего от правильной работы службы DNS.

8.1.2. Компьютер под управлением Windows NT 4.0

Система Microsoft Windows NT 4.0 Workstation использует для нахождения контроллера домена службу Windows NT Locator, которая работает с именами NetBIOS.

1. После того как пользователь введет свои регистрационные данные, вызывается служба Netlogon.
2. Служба Netlogon запрашивает службу Windows NT Locator. Последняя ищет запись контроллера домена, используя NetBIOS-имя домена.

3. Если в сети работает служба WINS, Windows NT Locator запрашивает запись контроллера домена у нее. Если служба WINS недоступна, Windows NT Locator посылает в сеть широковещательный запрос и в качестве последнего средства просматривает файл LMHOSTS.
4. Найденная запись передается службе Netlogon, которая проводит дальнейшие действия.

Отсюда становится ясно, что, если в сети есть хотя бы один узел с операционной системой более ранней версии, чем Windows 2000 Professional, необходимо дополнительно к службе DNS установить службу WINS. Только после этого вы будете уверены, что все процессы в сети происходят правильно.

У вас может возникнуть вопрос: почему служба WINS так необходима, если контроллер домена можно найти и по широковещательному запросу? Дело в том, что такие запросы не проходят через маршрутизатор. Если контроллер домена находится в головном офисе, а клиентский компьютер — в подсети подразделения, связанной с головным офисом через шлюз, то по широковещательному запросу контроллер домена найден не будет.

8.2. Разрешение имен службой WINS

Поскольку на практике можно достаточно часто встретить пример, когда в сетях, кроме системы Windows XP Professional или Windows 2000 Professional встречаются операционные системы Windows 9x или Windows NT 4.0, рекомендуется устанавливать в подобной сети службу WINS.

Служба WINS устанавливается как компонент серверных операционных систем, а на компьютерах-клиентах нужно настроить параметры подключения.

8.2.1. Установка службы WINS

Для установки службы WINS на сервере проделайте следующее:

1. Зарегистрируйтесь на сервере SRVR001 как Администратор. В главном меню выберите **Панель управления → Установка или удаление программ.**
2. В левой части открывшегося окна **Установка или удаление программ** выберите пункт **Установка компонентов Windows.**
3. В окне Мастера компонентов Windows выберите **Сетевые службы (Networking Services)**, а затем нажмите кнопку **Состав.**
4. Установите флажок **Служба Windows Internet Name Service (WINS) (Windows Internet Name Service (WINS))** и затем поочередно нажмите кнопки **OK** и **Далее.**

5. В ходе установки службы WINS вы должны вставить установочный компакт-диск операционной системы Windows Server 2003. Установку закончите нажатием на кнопку **Готово.**

8.2.2. Настройка службы WINS

Вместе с сервером WINS устанавливается также консоль под названием WINS для управления этим сервером. Пока что в сети существует единственный сервер WINS и он не требует после установки никакой настройки. Однако мы можем просто посмотреть, как происходит управление данными, которые расположены в базе данных WINS.

Настройка сервера как клиента службы WINS

Настройка сервера как клиента службы WINS состоит из следующих этапов:

1. Вызовите окно свойств **Подключение по локальной сети** и откройте свойства **Протокол сети Интернет (TCP\IP)**.
2. В диалоговом окне **Протокол сети Интернет (TCP\IP) — свойства** нажмите кнопку **Дополнительно** и затем на вкладке **WINS** нажмите на кнопку **Добавить.**
3. Введите IP-адрес сервера SRVR001 (192.168.10.2) и нажатием на кнопку **Добавить** добавьте его. Закройте диалоговое окно нажатием на клавишу **OK.**
4. Закройте все диалоговые окна.

С этого момента сервер SRVR001 стал сам для себя клиентом службы WINS. Теперь он может как искать в базе данных WINS NetBIOS-имена, так и регистрировать в ней свои записи. Сейчас мы просмотрим эти записи.

Консоль WINS: просмотр содержимого базы данных

Просмотр содержимого базы данных WINS осуществляется с помощью соответствующей консоли:

1. В главном меню выберите **Администрирование → WINS.** Появится консоль WINS.
2. В левой части окна консоли щелкните по пункту **Состояние сервера.** Если все выполнено правильно, то в столбце **Состояние** в правой части окна должно появиться значение **отвечает** (рис. 8.3).
3. Далее в левой части окна разверните ветвь сервера (SRVR001) и щелкните по папке **Активные регистрации.**
4. Щелкните правой кнопкой мыши на строке **Активные регистрации** в левой части окна и из контекстного меню выберите команду **Отобразить записи.**

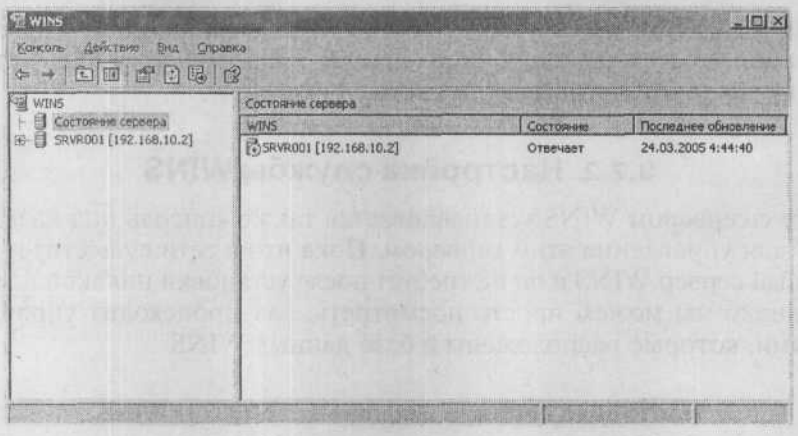


Рис. 8.3. Консоль управления сервером WINS

5. В диалоговом окне **Отобразить записи** можно задать фильтр, указывающий, какие именно записи требуется показать. Мы хотим отобразить все записи, поэтому нажмите кнопку **Найти.**

Примечание.

На вкладке **Сопоставление записей** можно задать фильтрацию записей по названиям. Здесь можно использовать подстановочные знаки (например,*). На вкладке **Владельцы записи** можно выбрать записи в зависимости от того, на каком сервере WINS они зарегистрированы, а на вкладке **Типы записей** можно задать выбор записей только определенного типа (Рабочая группа, Контроллер домена, Файловый сервер и т.п.).

Обратите внимание на записи типа **[1Ch] Контроллер домена** на рис. 8.4. Это и есть та запись, которую при регистрации пользователя разыскивает служба Windows NT Locator.

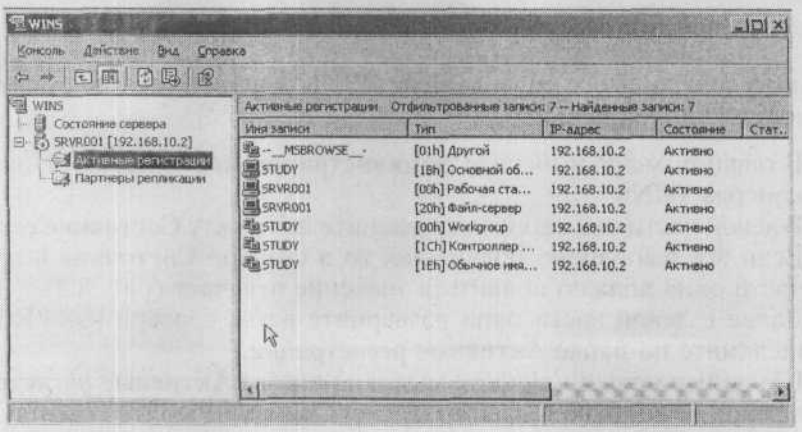


Рис. 8.4.

Сейчас база данных WINS содержит семь записей, которые зарегистрировал сервер SRVR001 сразу после того, как вы установили службу WINS.

Чтобы компьютер мог запросить службу WINS о необходимой информации, он должен быть клиентом WINS. Однако ни один из наших компьютеров этому условию не удовлетворяет, поскольку в однородных сетях с системами Windows 2000 и более поздними служба WINS не требуется. В тот момент, когда компьютер становится клиентом службы WINS, он регистрирует свои записи в базе данных, а в дальнейшем перерегистрирует их при каждом включении. Служба WINS разрешает NetBIOS-имена динамически и не требует задавать никаких данных вручную.

В заключение хочу напомнить, что служба WINS нужна только тогда, когда в сети есть узел под управлением ОС Windows версии более ранней, чем Windows 2000. В противном случае эта служба будет обременять сеть без всякой пользы.

Практический пример: устаревший компьютер в филиале (или как обойтись без установки WINS)

Рассмотрим пример, когда можно обойтись без установки службы WINS. Пусть у некоторой компании есть офис, все компьютеры в котором работают под управлением Windows XP, и склад, где стоит единственный компьютер-клиент с системой Windows NT 4.0 Workstation. Все серверы под Windows Server 2003 стоят в офисе. Склад присоединен к сети линией со скоростью 56 Кб.

С точки зрения топологии такая сеть выглядит как две подсети, между которыми работает маршрутизатор.

Что происходит при попытке регистрации в домене пользователя со склада? Служба Windows NT Locator ищет NetBIOS-имя контроллера домена. Сервера WINS в сети нет, широковещательный запрос не проходит через маршрутизатор, поэтому Windows NT Locator прибегает к последнему средству — просмотру файла LMHOSTS. Если этого файла на клиентском компьютере нет, то поиск домена завершается неудачно и регистрации не происходит.

Существуют два решения этой задачи.

РЕШЕНИЕ А. Установить службу WINS на одном из серверов офиса и сконфигурировать все компьютеры сети, включая компьютер на складе, как клиентов WINS. Работать это будет, но складской компьютер будет занимать линию регистрацией в службе WINS своих NetBIOS-имен каждый раз при включении и WINS-запросами в течение дня. Очевидно, что линии 56 Кб для одного компьютера будет достаточно, но если на складе

стоят десятки компьютеров, то могут возникнуть проблемы. Ведь линия связи между подсетями протянута ради работы коммерческих приложений, которую лишняя нагрузка может нарушить.

Недостатком этого решения является также то, что в сети будет работать дополнительная служба, настройка и поддержание которой — это работа, требующая дополнительной оплаты.

РЕШЕНИЕ Б. Складскому компьютеру нужно связываться не со всеми компьютерами в офисе, а только с серверами и, может быть, с некоторыми клиентами. Эти сервера и клиенты можно прописать в файле `%systemroot%\system32\drivers\etc\LMHOSTS`, который будет выглядеть примерно так:

```
192.168.10.2     SRVR001 #PRE    #DOM:STUDY
192.168.10.17    PC001
192.168.10.18    PC002
```

После этого складской компьютер сможет найти сервер SRVR001, управляющий доменом с NetBIOS-именем STUDY (запись с ключевым словом #DOM), то есть пользователь со склада сможет зарегистрироваться в домене. После регистрации этот компьютер сможет обмениваться данными только с сервером и рабочими станциями PC001 и PC002.

Сравнение стоимости и трудоемкости этих двух решений предоставляю вам самим.

8.3. Служба DHCP: раздача IP-адресов в крупной сети

8.3.1. Общая информация

Сеть любого предприятия рано или поздно разрастается. Это случается по разным причинам. К ним относятся как рост компании и необходимость расширять штат (новые клиентские места и наращивание мощи обслуживающих сеть серверов), так и неосведомленность администратора о правильной настройке служб и приложений сети и как следствие использование большего количества серверов, чем это необходимо. Цель этого и последующих параграфов данной главы — научить администратора не бояться роста сети и показать, как настроить протокол IP на большом количестве узлов.

Первый вопрос, касающийся сети (конфигурация параметров протокола TCP\IP) решается во время установки любого компьютера. В системах Windows 2000 и более поздних во время установки необходимо выбрать

стандартную настройку или же задать конкретные службы, протоколы и их настройки (собственные настройки).

8.3.2. Типы адресации протокола IP

Если вы выбираете при установке сетевых компонентов стандартный вариант, то установятся основные три сетевых компонента — **Служба доступа к файлам и принтерам сетей Microsoft**, **Клиент для сетей Microsoft** и **Протокол Интернета (TCP\IP)**, для которого будет выбран динамический тип адресации. Если вы хотите поменять какие-то настройки (в том числе и конфигурацию IP-адреса), это придется делать вручную.

Статическая адресация

Назначение адресов вручную, или статически, применяется в небольших сетях. При наличии десятка узлов оно выгодно тем, что регистрация в сети происходит быстрее и администратор имеет возможность отслеживать работу компьютеров по их IP-адресам. На вопрос, с какого количества узлов оно перестает быть выгодным, не существует однозначного ответа. Все зависит от квалификации администратора и физического расположения компьютеров: чем больше в сети физически удаленных узлов, тем больше времени потребуется на то, чтобы обойти их все и вручную назначить или сменить IP-адреса.

Имейте в виду, что в ОС Windows 2000 и Windows NT 4.0 изменение сетевых компонент может производить только администратор компьютера. В Windows XP Professional и Windows Server 2003 такими полномочиями обладают и члены группы Network Configuration Operators.

Динамическая (автоматическая) адресация

Если вы настроили новый, скажем, вторичный сервер DNS, то вам придется прописать его IP-адрес в настройках протокола TCP/IP на всех узлах сети. При статической адресации вас ждет масса работы: придется подходить к каждому компьютеру, сгонять пользователя, регистрироваться как локальный администратор и менять параметры протокола TCP/IP, стараясь не допустить опечатки. Большинству администраторов, особенно крупных сетей, этот путь не подходит: выгоднее все сделать автоматически, охватив все узлы за один раз.

Чтобы автоматическая настройка параметров протокола IP работала, в сети должен работать сервер DHCP (Dynamic Host Configuration Protocol). DHCP называют и службой, и протоколом, и оба названия верны.

8.4. Установка и настройка службы DHCP

Сервер DHCP слушает запросы клиентов на автоматическую настройку протокола IP и отвечает на них предложением набора конфигурационных параметров. Клиентский запрос может быть либо требованием полной настройки, либо просьбой о разрешении продолжать использовать имеющуюся конфигурацию.

Получение клиентом IP-адреса от сервера DHCP называется арендой адреса. Сервер DHCP имеет в своем распоряжении некоторый диапазон IP-адресов (его называют пулом IP-адресов), которые он может предоставлять в аренду. При выключении клиентский компьютер возвращает арендованный адрес обратно серверу, и этот адрес снова становится разрешен к выдаче.

Если в сети работает служба DHCP, то администратор не рискует ошибиться при настройке протокола IP на отдельных компьютерах или случайно назначить им одинаковые IP-адреса.

Чтобы перевести сеть с ручной адресации на динамическую, нужно не только установить и настроить сервер DHCP, но и изменить способ адресации протокола IP на всех узлах сети.

8.4.1. Установка службы DHCP

Служба DHCP устанавливается как компонент серверной операционной системы Windows Server 2003. Ее можно установить как на отдельном сервере, так и на одном из уже имеющихся. В нашей небольшой сети использование нескольких серверов пока нецелесообразно, и мы будем устанавливать DHCP все на том же SRVR001.

1. Зарегистрируйтесь на сервере SRVR001 как Администратор. В главном меню выберите **Панель управления → Установка или удаление программ.**
2. В левой части открывшегося окна **Установка или удаление программ** выберите пункт **Установка компонентов Windows.**
3. В окне Мастера компонентов Windows выберите **Сетевые службы (Networking Services),** а затем нажмите кнопку **Состав.**
4. Из списка сетевых служб выберите **Протокол динамической конфигурации хоста (Dynamic Host Configuration Protocol DHCP)** и нажмите кнопку **OK.**
5. Нажмите кнопку **Далее** и подождите установки службы DHCP. Вам может понадобиться вставить установочный компакт-диск с операционной системой Windows Server 2003.
6. Нажатием клавиши **Готово** закончите установку.

После установки службы DHCP в группе команд **Администрирование** меню **Пуск** появится пункт **DHCP**, щелчок по которому вызывает консоль управления DHCP. Если все установлено правильно, то в левой части окна консоли должен быть указан сервер `srvr001.study.local` вместе со своим IP-адресом. Развернув ветвь этого сервера, в правой части окна в столбце **Состояние** вы увидите значение **Не авторизован** (рис. 8.5). Это значит, что служба DHCP успешно установлена, тем не менее ни один IP-адрес выдать она еще не готова. Поэтому необходимо заняться ее дальнейшей настройкой.

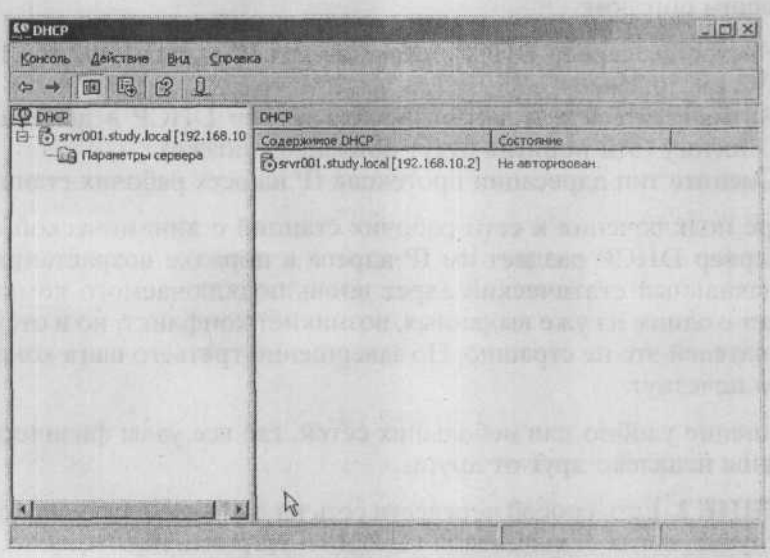


Рис. 8.5. *Консоль управления сервером DHCP*

8.4.2. Настройка службы DHCP

Для настройки службы DHCP необходимо указать как общие, одинаковые для всех узлов, параметры сети (маску подсети, адреса основного шлюза, серверов DNS и WINS и т.п.), так и диапазон адресов, предоставляемых в аренду. Назначение пула адресов следует продумать особенно тщательно.

Мы договорились, что в нашей сети адреса от 192.168.10. 2 до 192.168.10.16 предназначены для статической адресации серверов и другого оборудования, а остаток — с 192.168.10.17 до 192.168.10.254 — для компьютеров-клиентов. Что произойдет, если выделить пул от 192.168.10.17 до 192.168.10.254? У нас уже есть компьютер с адресом 192.168.10.17. Сервер DHCP способен определить, не занят ли уже адрес, который он собирается предоставить в аренду, но для этого компьютер

с этим адресом должен быть в данный момент включен и присоединен к сети. Если наш PC001 сейчас выключен, то после его включения в сети окажется два узла с одинаковыми адресами и возникнет конфликт.

Способы перехода со статической адресации на динамическую

РЕШЕНИЕ 1. Изменение IP-адресации можно оставить на вечернее время или выходные дни, когда конфликт IP-адресов не помешает работе ни одного пользователя сети, а затем провести всю настройку сразу следующим образом:

1. Настройте сервер DHCP, назначив пул IP-адресов 192.168.10.17 до 192.168.10.254.
2. Активируйте пул и авторизируйте сервер DHCP в домене Active Directory (эти понятия будут объяснены позже).
3. Смените тип адресации протокола IP на всех рабочих станциях.

По мере подключения к сети рабочих станций с динамической адресацией сервер DHCP раздает им IP-адреса в порядке возрастания. Если первоначальный статический адрес вновь подключаемого компьютера совпадет с одним из уже выданных, возникнет конфликт, но в отсутствие пользователей это не страшно. По завершении третьего шага конфликты адресов исчезнут.

Это решение удобно для небольших сетей, где все узлы физически расположены недалеко друг от друга.

РЕШЕНИЕ 2. Есть способ перевести сеть на динамическую адресацию и в том случае, когда общесетевой выходной устроить невозможно. Чтобы провести изменение адресации в рабочее время, причем не доводя до конфликта IP-адресов, нужно проделать следующее:

1. Настройте сервер DHCP, назначив пул IP-адресов с 192.168.10.x до 192.168.10.254, где x — первый незанятый IP-адрес в сети.
2. Активируйте пул и авторизируйте сервер DHCP в домене Active Directory.
3. Смените тип адресации протокола IP на всех рабочих станциях, последовательно расширяя пул в направлении меньших IP-адресов.

Когда очередной узел переключается на динамическую адресацию, сервер DHCP выдает ему первый свободный адрес из пула. Теперь его бывший статический адрес свободен и его можно добавить в пул.

При этом подходе следует принять во внимание следующие моменты:

- Для третьего шага узлы сети нужно разбить на блоки смежных IP-адресов и перенастраивать компьютеры в порядке убывания статического адреса. То есть если первым свободным адресом является

192.168.10.84, то нужно сменить тип адресации у узла 192.168.10.83, затем у 192.168.10.82 и так далее до 192.168.10.79, после чего расширить пул вниз до 192.168.10.79.

- Размер блока нужно выбирать с учетом того, что в момент непосредственно перед расширением пула группа из N компьютеров занимает 2*N адресов (N действующих динамических и N бывших, не возвращенных в пул). Чем крупнее сеть, тем меньшими должны быть блоки.

Вариантом второго способа является использование дополнительных возможностей сервера DHCP — например, зарезервированного диапазона адресов.

РЕШЕНИЕ 3. Самый радикальный подход к смене типа адресации — это переход на другую подсеть. Сервер DHCP будет выдавать новые адреса из диапазона, например, 192.168.11.0/24, и конфликта со старыми адресами не возникнет.

В нашей сети мы воспользуемся вторым способом.

Настройка сервера DHCP

Чтобы настроить сервер DHCP, вам нужно проделать следующую последовательность действий:

1. Запустите консоль управления DHCP.
2. В левой части окна консоли щелкните правой кнопкой мыши по серверу `srvr001.study.local` и из контекстного меню выберите команду **Создать область**. По этой команде запустится Мастер создания области. Нажмите **Далее**.
3. В диалоговом окне **Имя области** введите название области (например, «Main office») и ее описание («Рабочие станции главного офиса»). Нажмите **Далее**.
4. В диалоговом окне **Диапазон IP-адресов** введите в поле **Начальный IP-адрес** первый незанятый адрес в вашей подсети (например, 192.168.10.26), а в поле **Конечный IP-адрес** — значение 192.168.10.254. Поля маски будут заполнены по умолчанию текущей маской сети (в нашем случае 24\255.255.255.0). Нажмите **Далее**.
5. В диалоговом окне **Добавление исключений** оставьте все значения пустыми и нажмите **Далее**.
6. В диалоговом окне **Срок действия аренды адреса** оставьте значение по умолчанию и нажмите **Далее.**
7. В диалоговом окне **Настройка параметров DHCP** выберите **Да, настроить эти параметры сейчас** и нажмите **Далее.**
8. В диалоговом окне **Маршрутизатор (основной шлюз)** не вводите ничего, а нажмите **Далее.**

9. В диалоговом окне **Имя домена и DNS-серверы** оставьте поле **Родительский домен** пустым, а в поле **IP-адрес** введите адрес 192.168.10.2. Затем нажмите кнопку **Добавить** и продолжите нажатием кнопки **Далее.**
10. В диалоговом окне **WINS-серверы**, если вы установили сервер WINS на SRVR001, введите в поле **IP-адрес** адрес 192.168.10.2 и нажмите кнопку **Добавить.** Нажмите **Далее**.
11. В диалоговом окне **Активировать область** отметьте поле **Нет, я активирую эту область позже** и нажмите **Далее**
12. Завершите работу мастера нажатием на кнопку **Готово.**

Проверьте, правильно ли вы задали параметры области, по консоли DHCP (рис. 8.6):

- В списке **Пул адресов** вы должны увидеть введенный диапазон IP-адресов (192.168.10.26 до 192.168.10.254).
- В списках **Арендованные адреса** и **Резервирование** не должно быть ни одного значения.
- В списке **Параметры области** должно быть три параметра: **006 DNS-серверы, 044 WINS\NBNS-серверы** и **046 Тип узла WINS\NBT**.

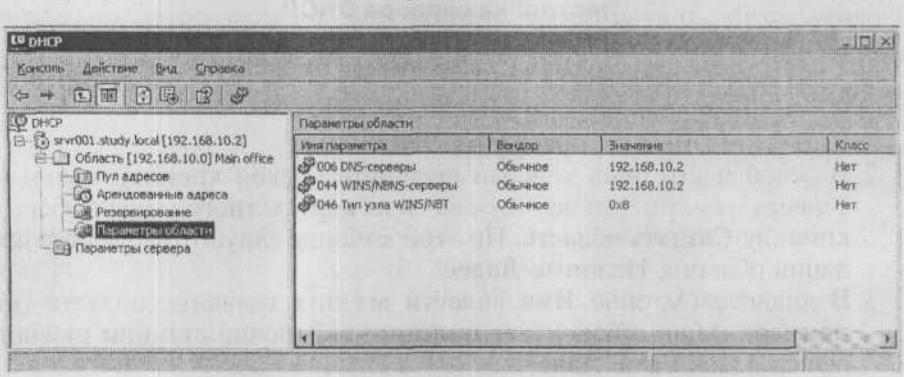


Рис. 8.6. *Параметры области сервера DHCP*

Если все в порядке, можно провести активацию области. Щелкните правой кнопкой мыши по области «Main office» в левой части окна консоли и из контекстного меню выберите команду **Активировать**. После ее выполнения из метки области исчезнет красная стрелка, отмечающая неактивные области.

Авторизация сервера DHCP в Active Directory

Несмотря на то, что все уже настроено, наш сервер DHCP еще не готов обслуживать клиентов. Сначала необходимо авторизовать его в домене Active Directory.

В сети может одновременно работать несколько серверов DHCP. Если они настроены так, чтобы выдавать адреса из одного и того же диапазона, то в сети быстро возникнет хаос: сервер DHCP учитывает только те IP-адреса, которые выдал сам, и предоставляет клиентам уже занятые другими адреса. Обычно администраторы создают эту аварийную ситуацию не умышленно, а в ходе экспериментов по улучшению обслуживания сети. Для настройки и запуска сервера DHCP достаточно полномочий администратора конкретного сервера.

Служба каталога Active Directory имеет возможность воспрепятствовать запуску «лишних», непредусмотренных серверов DHCP. Эта возможность и называется авторизацией: работать в сети будет разрешено только тем серверам DHCP, которые явно авторизованы администратором предприятия. Технически авторизация — это создание записи в базе данных активного каталога. Каждый сервер DHCP при попытке запуска проверяет наличие этой записи: если она есть, сервер запускается и начинает раздавать IP-адреса; если она отсутствует, значит, сконфигурированная для этого сервера область адресов уже активна, и он не запускается.

Если сеть предприятия организована в единственный домен, то для проведения авторизации вам хватит полномочий, предоставляемых членством в группе администраторов домена (Domain Admins). Если доменов несколько, то вы должны быть членом группы администраторов предприятия (Enterprise Admins).

Порядок авторизации сервера DHCP в домене Active Directory состоит из следующих этапов:

1. Зарегистрируйтесь на сервере SRVR001 как член группы Enterprise Admins (наша учетная запись Администратор входит в эту группу) и запустите консоль DHCP.
2. В левой части окна консоли щелкните правой кнопкой мыши по `srvr001.study.local` и из контекстного меню выберите команду **Авторизовать** (рис. 8.7).

После обновления изображения в окне консоли DHCP красная стрелка у значка сервера должна превратиться в зеленую.

Примечание.

Если вы хотите определить, какие серверы DHCP уже авторизованы, щелкните правой кнопкой мыши по значку DHCP в левой части консоли и выберите из контекстного меню команду **Управлять авторизованными серверами**. В появившемся диалоговом окне вы увидите список всех авторизованных серверов и сможете добавить к нему новый сервер DHCP или удалить имеющийся.

К сожалению, гарантированно защититься от появления в сети несанкционированного DHCP-сервера невозможно. Способ авторизации будет работать только тогда, когда:

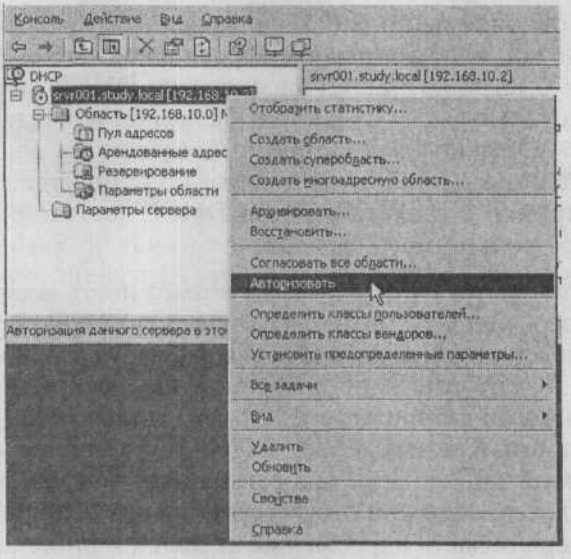


Рис. 8.7. *Авторизация сервера DHCP в домене Active Directory*

1. сеть организована в домен Active Directory (то есть в домен под управлением ОС Windows 2000 Server или Windows Server 2003);
2. все сервера DHCP установлены на компьютерах с ОС Windows 2000 Server или Windows Server 2003, являющихся членами домена.

А в следующих, довольно распространенных, обстоятельствах авторизация не принесет никакой пользы:

- Сервер DHCP установлен на компьютере под управлением Windows NT 4.0 Server или ОС UNIX, входящем в домен Active Directory.
- Сервер DHCP установлен на компьютере под управлением Windows 2000 Server, не входящем в домен Active Directory.
- Сервер DHCP установлен на компьютере под управлением Windows 2003 Server, который является членом домена Windows NT 4.0.
- Одна и та же подсеть IP организована в два независимых леса Active Directory, в каждом из которых работает авторизованный сервер DHCP.

В домене Windows 2003 Server авторизация серверов DHCP обязательна. Неавторизованный сервер работать не будет, а в системном журнале (**Пуск → Панель управления → Администрирование → Просмотр событий**) появится сообщение об ошибке с кодом 1046. Успешная авторизация сервера также отражается в системном журнале — как уведомление с кодом 1044.

8.4.3. Перевод рабочих станций на динамическую адресацию

В пункте 8.4.2 мы условились, что первый незанятый IP-адрес в нашей сети — это 192.168.10.26. Значит, последним клиентским компьютером, на котором мы настроили протокол IP, был PC009 со статическим адресом 192.168.10.25. С него и нужно начинать перенастройку.

1. Зарегистрируйтесь на PC009 как локальный администратор и в свойствах протокола TCP/IP смените адресацию протокола IP на автоматическую (рис. 8.8).

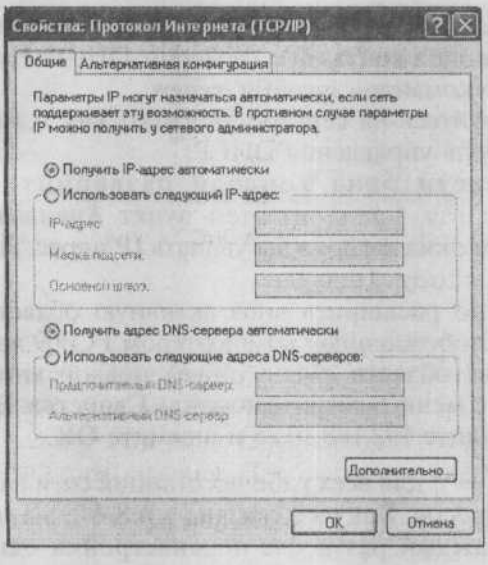


Рис. 8.8. *Назначение автоматического получения IP-адреса*

2. Откройте окно командной строки и командой **ipconfig /all** проверьте, получил ли компьютер PC009 новый IP-адрес от сервера DHCP. Ответ команды должен выглядеть примерно так:

```
C:\ Documents and Settings\Administrator.STUDY> ipconfig /all
Настройка протокола IP для Windows
Имя компьютера : pc009
Основной DNS-суффикс  : study.local
Тип узла  : неизвестный
IP-маршрутизация включена  : нет
WINS-прокси включен : нет
Порядок просмотра суффиксов DNS  : study.local
Подключение по локальной сети – Ethernet адаптер:
DNS-суффикс этого подключения    : study.local
```

```
Описание  : AMD PCNET Family PC Ethernet Adapter
Физический адрес  : DC-50-56-40-00-33
Dhcp включен : да
Автонастройка включена : да
IP-адрес  : 192.168.10.26
Маска подсети  : 255.255.255.0
Основной шлюз
DHCP-сервер  : 192.168.10.2
DNS-серверы  : 192.168.10.2
Аренда получена  : 8 октября 2005 16:44:15
Аренда истекает  : 16 октября 2005 16:44:15
```

Если вы видите IP-адрес, равный 0.0.0.0, значит, компьютер PC009 еще не установил контакта с сервером DHCP. Нужно подтолкнуть его вручную командой **ipconfig /renew**.

3. Зарегистрируйтесь на сервере SRVR001 как Администратор и откройте консоль управления DHCP.
4. В левой части окна консоли разверните ветвь сервера `srvr001.study.local` и затем пункт **Арендованные адреса**. В правой части окна вы должны увидеть IP-адрес, выданный компьютеру `pc009.study.local`.
5. Теперь нужно расширить вниз активную область адресов, включив в нее освобожденный компьютером PC009 адрес 192.168.10.25. Щелкните на области «Main office» правой кнопкой мыши и из контекстного меню выберите команду **Свойства**. В поле **Начальный IP-адрес** введите 192.168.10.25 и нажмите **OK**.

Повторите шаги 1 — 5 для всех рабочих станций сети в порядке убывания статических IP-адресов. Как уже сказано в п.8.4.2, вы можете расширять пул адресов не каждый раз после перенастройки одного клиентского компьютера, а через несколько обладателей подряд идущих статических адресов.

8.4.4. Адресация серверов

Ввиду той роли, которую в сети играют серверы, им нужно назначать статические адреса. Хотя протокол DHCP разрабатывался так, чтобы по возможности выдавать одному и тому же клиенту один и тот же адрес, рассчитывать на это нельзя. Если адрес сервера внезапно меняется, то в сети могут возникнуть проблемы.

У серверов нашей сети с самого начала адреса были назначены вручную, и менять здесь ничего не требуется. Нужно проследить только за тем, чтобы не включать в пул адресов, отдаваемых в аренду, IP-адреса, предназначенные для серверов.

8.4.5. Адресация принтеров и подобных устройств

Сетевыми называются те устройства, которые подключены непосредственно к локальной сети, а не к какому-либо отдельному компьютеру через USB или параллельный порт. Типичные представители таких устройств — сетевые принтеры. Для таких устройств выгодно иметь постоянный адрес, как у серверов, но в то же время назначать этот адрес централизованно, как рабочим станциям. Сервер DHCP может совместить эти требования с помощью механизма резервирования IP-адресов.

К принтерам мы еще вернемся в 14 главе, но резервирование адресов рассмотрим сейчас. Цель резервирования состоит в том, чтобы гарантировать, что определенный клиент DHCP (устройство или обычный компьютер) всегда и при любых обстоятельствах будет получать в аренду один и тот же IP-адрес. Технически резервирование — это привязка определенного IP-адреса к физическому адресу сетевого интерфейса клиента (MAC-адрес, Media Access Control).

Чтобы зарезервировать IP-адрес 192.168.10.16 за принтером с MAC-адресом 00-00-12-cc-b9-a0, выполните следующие действия:

1. Зарегистрируйтесь на сервере SRVR001 как Администратор и откройте консоль управления DHCP.
2. В левой части окна консоли разверните ветвь сервера `srvr001.study.local`, затем область «Main office», затем щелкните по значку **Резервирование** правой кнопкой мыши.
3. Выберите из контекстного меню команду **Новое резервирование**. В появившемся диалоговом окне введите название и краткое описание резервирования, в поле **IP-адрес** введите 192.168.10.16, а в поле **MAC-адрес** — строку «000012ccb9a0». В области поддерживаемых типов оставьте предложенное значение «Оба» и нажмите кнопку **Добавить**.

Теперь, если вы развернете значок **Арендованные адреса**, среди выданных в аренду адресов будут перечислены и зарезервированные. Несмотря на то, что мы зарезервировали адрес, не входящий в пул, по запросу от клиента, однозначно идентифицируемого своим MAC-адресом, этот IP-адрес будет ему предоставлен.

8.5. Сбой службы DHCP

Как и любая другая служба, DHCP может выйти из строя, и администратору нужно подготовиться к этому событию так, чтобы минимизировать возможный ущерб сети. Вы уже знаете, что работающего запасного

DHCP-сервера с таким же пулом адресов в сети быть не может. В этом параграфе мы рассмотрим, какие средства защиты от сбоев реализованы в протоколе DHCP вместо этого.

8.5.1. Как клиент получает IP-адрес в отсутствие сервера DHCP

Клиентский компьютер, настроенный на автоматическое получение адреса, сразу после включения посылает широковещательный запрос «кто я?». Если какой-нибудь сервер DHCP отзовется на этот запрос, то клиент принимает от него IP-адрес и начинает нормальную работу в сети. Если ни один сервер DHCP не отозвался, то клиент делает еще несколько попыток через определенные интервалы времени, а потом назначает себе адрес сам. Каким образом он это сделает, зависит от конкретной операционной системы.

Windows 9x и Windows NT

Компьютер с операционной системой, более ранней, чем Windows 2000 (исключая Windows 98 SE и Windows ME), не получив отклика от сервера DHCP, остается без IP-адреса. Если вы введете в командной строке команду **ipconfig**, то увидите IP-адрес 0.0.0.0. В результате этот компьютер работать в сети по протоколу TCP/IP не сможет.

Windows 98 и Windows 2000

ОС семейства Windows 2000, а также системы Windows 98 SE и Windows ME, в случае недоступности сервера DHCP прибегают к средству APIPA (Automatic Private IP Addressing). APIPA представляет собой механизм, обеспечивающий клиентам небольших сетей возможность автоматического присвоения адресов из подсети 169.254.0.0/16.

Компьютер просто случайным образом выбирает адрес из диапазона 169.254.x.x и устанавливает маску 255.255.0.0. В этом диапазоне доступно 65534 адреса, поэтому риск того, что два компьютера выберут два одинаковых адреса, минимален. Чтобы полностью исключить риск конфликта, клиент, выбрав адрес, посылает широковещательный запрос, выясняя, не занят ли уже этот адрес. Клиент повторяет попытки присвоить себе адрес до тех пор, пока не наткнется на свободный.

Компьютер, получивший адрес с помощью APIPA, имеет возможность связываться с другими компьютерами в пределах своей физической подсети.

Windows XP и Windows Server 2003

В операционных системах клиентского семейства Windows XP и серверного Windows Server 2003 процедура самоприсвоения адреса была еще более усовершенствована. Если при настройке протокола TCP/IP выбрано автоматическое получение адреса, то в диалоге свойств протокола TCP/IP появляется дополнительная вкладка **Альтернативная конфигурация**.

На этой вкладке, установив переключатель в положение **Настроенные пользователем**, можно указать параметры протокола IP так же, как при статической настройке. Другое положение этого переключателя — **APIPA** — указывает компьютеру в отсутствие DHCP-сервера поступать так же, как компьютеры под управлением Windows 2000.

8.5.2. Как бы это выглядело в нашей сети

Если бы в нашей сети вышла из строя служба DHCP, рабочие станции под управлением Windows XP Professional назначили бы себе IP-адреса из подсети 169.254.0.0/16. Остальные устройства, не поддерживающие механизм APIPA (например, принтеры), оказались бы без IP-адреса и были бы недоступны по сети. Сервер SRVR001 настроен на статическую адресацию, поэтому сбой сервера DHCP его, казалось бы, не касается. Но он использует маску подсети 255.255.255.0, а клиенты назначили бы себе маску 255.255.0.0, оказавшись тем самым в другой подсети. Как они будут разрешать имена?

В главе 6 вы узнали, что при невозможности найти узел сети по имени при помощи службы DNS (она установлена на сервере SRVR001, который еще нужно найти) ОС Windows продолжает поиск по имени NetBIOS, посылая широковещательный запрос. Такой запрос может принести ответ только в пределах подсети, то есть клиенты смогут найти друг друга, но не сервер.

Значит ли это, что механизм APIPA не слишком полезен, раз он не может восстановить главную функцию обычной сети — коммуникацию клиентов с сервером? Нет, не значит. Он очень полезен в сетях равноправных узлов (peer-to-peer), где ни один узел не настроен на статическую адресацию.

Если, например, вы устанавливаете небольшую сеть, состоящую из четырех компьютеров под управлением Windows XP Professional, то можете при установке операционной системы оставить конфигурацию протокола IP по умолчанию, то есть настроенной на автоматическое получение адреса, а сервер DHCP вообще не устанавливать. Тогда компьютеры-клиенты сами назначат себе IP-адреса и, оказавшись в одной и той же подсети, будут спокойно общаться по ним.

А альтернативная конфигурация протокола TCP/IP — это решение для владельцев ноутбука, которым нужно подключаться к разным сетям, причем одна из них использует сервер DHCP, а другая нет. Если настроить ноутбук на автоматическое получение адреса, а статические параметры протокола TCP/IP прописать на вкладке **Альтернативная конфигурация**, то такой ноутбук сможет без перенастройки работать в обеих сетях.

8.5.3. Страховка на случай сбоя службы DHCP

Наша (малая) сеть

Для быстрого восстановления функциональности сети в случае сбоя сервера DHCP в первую очередь необходимо иметь в распоряжении запасной сервер. Для многих предприятий это очень ограничивающий фактор, поэтому они вынуждены обходиться без страховки. Обойдемся и мы, поскольку устанавливать дополнительный сервер мы не планируем.

Крупные сети

Если в сети предприятия несколько серверов, то на одном из них можно установить дополнительный сервер DHCP, разбив пул арендуемых адресов на две области (корпорация Microsoft рекомендует разбивать в отношении 80/20).

Для нашей сети это означало бы, что первый сервер DHCP выдает адреса из диапазона 192.168.10.17 — 192.168.10.207, а второй — от 192.168.10.208 до 192.168.10.254. Большая область отводится для штатного режима работы сети, меньшая — для аварийного. 20-процентный запас считается достаточным, потому что на момент сбоя многие компьютеры будут иметь уже выданный IP-адрес. Резервирование нужно настроить на обоих серверах.

8.6. Итоги

В однородной сети, объединяющей только компьютеры под управлением Windows 2000/XP/2003, разрешение имен выполняет служба DNS. Если на некоторых узлах сети стоят операционные системы более ранних версий, использующие имена NetBIOS, то понадобится установить дополнительную службу для разрешения этих имен.

Системным решением является в таком случае установка и настройка службы WINS. В некоторых случаях (например, несколько старых ком-

пьютеров в удаленном подразделении) может оказаться достаточно настроить файлы LMHOSTS.

Настройку протокола IP существенно облегчает служба (протокол) DHCP. Эта служба является компонентом ОС Windows Server 2003 и Windows 2000 Server и обеспечивает автоматическую адресацию всех устройств, работающих по протоколу IP.

Чтобы сервер DHCP начал обслуживать клиентов, он должен пройти авторизацию в домене Active Directory. В общем случае для авторизации сервера нужны полномочия члены группы администраторов предприятия (Enterprise Admins), но иногда достаточно прав члена группы администраторов домена (Domain Admins).

В тех сетях, где некоторым узлам адреса назначаются вручную, при установке службы DHCP нужно действовать осторожно. Служба DHCP не способна определить, какие адреса уже используются в сети, если их выдавала не она, поэтому пул арендуемых адресов следует настраивать так, чтобы исключить выдачу адреса, совпадающего с одним из статических.

Клиент службы DHCP в составе ОС Windows 2000/XP имеет возможность работать в аварийном режиме, в отсутствие сервера DHCP. Он самостоятельно назначает своему компьютеру адрес, случайно выбирая его из подсети 169.254.0.0/16. В результате клиентские компьютеры могут общаться между собой, но не со статически адресованными серверами.

ОС Windows XP Professional, в отличие от Windows 2000, предоставляет возможность двойной настройки протокола IP: при выборе автоматического получения адреса на вкладке **Альтернативная конфигурация** можно указать статический набор параметров, который вступает в силу тогда, когда сервер DHCP в сети не обнаружен.

В крупных сетях рекомендуется иметь несколько серверов DHCP, разделив между ними пул адресов в пропорции 80\20.

Состояние сети

В нашей сети появились службы WINS и DHCP, *установленные на сервере* SRVR001. Сервер DHCP авторизован в домене Active Directory и служит для автоматического назначения IP-адресов рабочим станциям. Рабочие станции стали также клиентами службы WINS.

Глава 9 Регистрация пользователей в домене. Управление учетными записями пользователей

К этому моменту наша сеть организована в домен. На сервере, который является контроллером домена, установлены и настроены службы, необходимые для работы сети. Целью этой системы с точки зрения администратора является как можно более простое управление, а с точки зрения предприятия — как можно больше удобств для работы пользователя.

Поскольку мы уже построили стабильную и работающую схему, можно «запускать» пользователей. Каждому пользователю мы создадим и настроим учетную запись, которая понадобится для работы в сети. В то же время познакомимся с инструментами, которые служат для управления пользователями в домене, посмотрим и на основные механизмы безопасности учетных записей пользователей.

9.1. Доменная учетная запись пользователя

Если пользователь хочет работать в сети, он должен зарегистрироваться на одном из узлов. Для этого необходимо наличие активной учетной записи и знание пользователем своих регистрационных данных — имени и пароля. Учетная запись служит также для регулирования полномочий пользователя — прав доступа к тем или другим ресурсам и возможности выполнять те или другие действия.

С учетными записями пользователей необходимо обращаться очень осторожно, потому что это одна из лазеек, через которые злоумышленник может проникнуть в сеть. Категорически не рекомендуется создавать общую запись для поочередной работы группы пользователей. Учетная запись, как зубная щетка, у каждого должна быть своя.

В домене с операционными системами Windows можно работать с двумя типами учетных записей: локальными и доменными. Разницу между ними, а также принципы работы с локальными учетными записями мы разобрали в 4 главе. В этой главе мы подробно рассмотрим управление доменными учетными записями.

9.2. Создание и настройка учетных записей

Если вы представите себе сеть с несколькими сотнями пользователей и подумаете, что вам придется создавать несколько сотен учетных записей, то ваше настроение может слегка испортиться. Правда, обычно учетные записи добавляются постепенно, по мере развития системы. Но даже если перед вами стоит задача добавить всего десяток новых учетных записей, не стоит торопиться.

Процесс создания одной записи может занять как несколько минут, так и несколько секунд. И если вам впоследствии потребуется ежедневно создавать несколько десятков новых записей, нужно продумать подход к их созданию уже сейчас.

Учетные записи можно создавать разными способами — и с помощью графического интерфейса, и запуском командного сценария, который будет считывать информацию из заранее подготовленного файла и записывать ее прямо в базу данных домена Active Directory. В каждой из возможностей есть как положительные, так и отрицательные стороны. Мы постараемся использовать лучшие из них.

9.2.1. Создание первой учетной записи

До сих пор мы работали под учетной записью Администратор. Это встроенная учетная запись, которая доступна сразу после установки домена. Эта запись предоставляет огромные полномочия, поэтому использовать ее для повседневной работы небезопасно. Сейчас мы создадим другую учетную запись, под которой и будем регистрироваться для обычной работы, а эту оставим только для некоторых административных задач, которые нельзя решить другим способом.

1. Зарегистрируйтесь на сервере SRVR001 как Администратор.
2. Запустите консоль **Active Directory — пользователи и компьютеры.**
3. Щелкните правой кнопкой мыши по значку **Пользователи (Users)** и из контекстного меню выберите **Создать → Пользователь.**
4. В диалоговом окне **Новый объект — Пользователь** введите в качестве имени и фамилии «Первый Пользователь» (рис. 9.1).

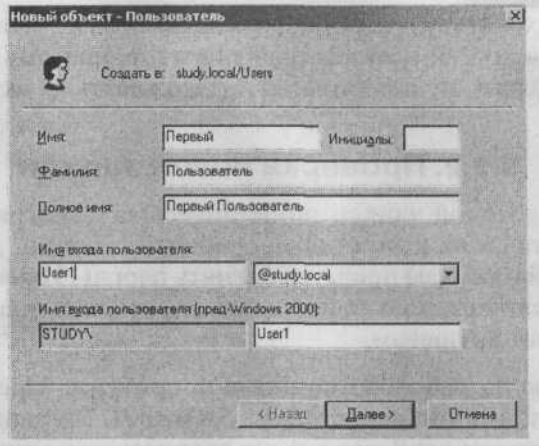


Рис. 9.1. *Создание доменной учетной записи*

5. В поле **Имя входа пользователя** введите, например, `User1`. Рекомендуется избегать использования в регистрационном имени символов кириллицы, поскольку не на каждом компьютере можно переключиться на русскую раскладку в ходе регистрации. Это же регистрационное имя будет автоматически введено и в поле **Имя входа пользователя (пред-Windows 2000)**. Данное значение можно изменить вручную, но обычно это не рекомендуется, так как пользователю придется запоминать лишнее имя. Нажмите **Далее.**
6. В поле **Пароль** и **Подтверждение** введите пароль, который будет применен при первой регистрации при помощи созданной записи. Настройка безопасности по умолчанию в домене с системой Windows Server 2003 довольно строгая: длина пароля должна быть не менее 7 символов, а пароль обязан быть сложным, то есть содержать символы не менее трех разновидностей из следующих: заглавная буква, строчная буква, цифра, специальный знак.
7. Оставьте установленным флажок **Требовать смену пароля при следующем входе в систему.** Это приведет к тому, что пароль будет знать только сам пользователь, а вы как администратор снимете с себя ответственность за доступ к чужим секретам. Остальные переключатели тоже оставьте в положении по умолчанию и нажмите **Далее.**
8. Отобразится общая информация о новом пользователе. После ее проверки нажмите кнопку **Готово**. Только сейчас учетная запись будет создана.
9. Вызовите окно свойств вновь созданной записи и просмотрите все вкладки (особенно вкладки **Адрес, Учетная запись, Профиль, Телефоны, Организация**), чтобы получить представление о других сведениях,

которые входят в учетную информацию пользователя. Эти сведения нужны для поиска пользователя в системе, поэтому имеет смысл задавать их сразу же и постоянно поддерживать их актуальность.

9.2.2. Проверка новой записи

После создания новой записи попытайтесь зарегистрироваться с помощью этой записи на какой-нибудь рабочей станции. До того, как вы увидите рабочий стол, вам придется сменить пароль. Успешное изменение пароля будет подтверждено сообщением на экране и новый пароль в тот же момент станет активным.

Завершите сеанс на рабочей станции и попробуйте зарегистрироваться под новой учетной записью на сервере SRVR001. Вы увидите сообщение «Локальная политика этой системы не дает возможности интерактивной регистрации». Дело в том, что вы создали запись с полномочиями рядового пользователя домена, который не должен работать за контроллером домена и иметь возможность что-либо менять в его настройках. Политика безопасности дает возможность зарегистрироваться на контроллере домена только некоторым группам пользователей.

9.2.3. Создание следующих учетных записей

Вы уже, должно быть, заметили, что только некоторые атрибуты учетной записи индивидуальны для каждого пользователя (например, телефонный номер или имя), другие же повторяются (например, у всех пользователей из отдела рекламы в поле **Отдел** на вкладке **Организация** будет стоять «Рекламный»). Это наводит на мысль о создании учетных записей по шаблону.

Наше учебное предприятие `Study` имеет следующую структуру: три директора, пять сотрудников в торговом отделе, три сотрудника в отделе маркетинга, три сотрудника на складе и один системный администратор. Время от времени на предприятии работает контрактник, которым может быть каждый раз другое лицо, но работу он выполняет примерно одну и ту же. Склад работает круглосуточно, остальные отделы — с 8 до 16 часов. Регистрационные имена сотрудников будут состоять из названия отдела и порядкового номера работника: `Manager1`, `Store3` и т.д.

Заготовим четыре шаблона — по одному для каждого отдела с количеством работников больше одного. Чтобы шаблоны были с первого взгляда узнаваемы в окне консоли **Пользователи и компьютеры** службы Active Directory, стоит назвать их именами отделов (`_Shop`, `_Marketing`, `_Warehouse` и `_Managers`). Знак подчеркивания добавлен для того, чтобы в алфавитном списке имена шаблонов стояли первыми.

Создание шаблона

Последовательность действий по созданию шаблона состоит из следующих этапов:

1. Зарегистрируйтесь на сервере SRVR001 как Администратор и запустите консоль **Active Directory — пользователи и компьютеры.** Удалите пробную запись «Первый пользователь».
2. Щелкните правой кнопкой мыши по значку **Пользователи (Users)** и из контекстного меню выберите **Создать → Пользователь.**
3. В диалоговом окне **Новый объект — Пользователь** введите в качестве имени «_Shop» (торговый отдел), а поле фамилии оставьте пустым.
4. В поле **Имя входа пользователя** введите `Shop` и нажмите кнопку **Далее.**
5. В поле **Пароль** и **Подтверждение** введите сложный пароль (не менее 8 символов, состоящий из заглавных и строчных букв, цифр или специальных знаков), оставьте установленным флажок **Требовать смену пароля при следующем входе в систему** и продолжите нажатием кнопки **Далее.**
6. Проверьте введенные сведения и создайте запись нажатием кнопки **Готово.**
7. Вызовите окно свойств вновь созданной записи и заполните все необходимые поля на вкладках **Адрес** и **Организация.**
8. На вкладке **Учетная запись** нажмите кнопку **Время входа** и оставьте синим период между 8 и 16 часами. Нажатием кнопки **OK** закройте диалоговое окно свойств.
9. Щелкните по созданной записи правой кнопкой мыши и из контекстного меню выберите команду **Отключить учетную запись.** Теперь под ней не сможет зарегистрироваться никто, даже зная пароль.

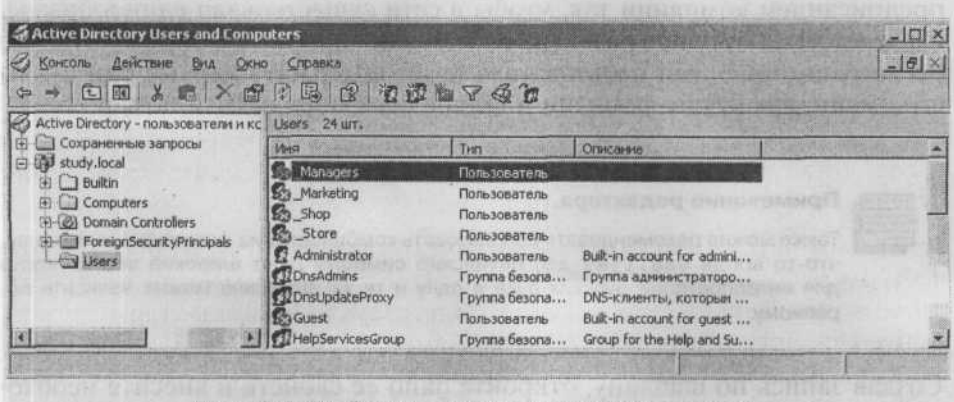


Рис. 9.2. *Шаблоны — отключенные учетные записи*

Таким же образом создайте шаблоны `_Marketing`, `_Store` и `_Managers` для отдела маркетинга, склада и дирекции. В шаблоне для склада установите круглосуточное время входа (п.8).

Теперь окно консоли **Active Directory — пользователи и компьютеры** выглядит так, как на рис. 9.2.

Создание учетной записи по шаблону

Создание учетной записи по шаблону производится следующим образом:

1. Щелкните по шаблону (`_Shop`) правой кнопкой мыши и из контекстного меню выберите команду **Копировать.** Появится диалог создания новой учетной записи.
2. Введите регистрационное имя `Shop1`, а в качестве имени и фамилии пользователя в этой книге мы будем использовать тоже `Shop1`. Нажмите кнопку **Далее.**
3. Задайте пароль для первого входа пользователя в систему, оставьте установленным флажок **Требовать смену пароля при следующем входе в систему** и снимите флажок **Отключить учетную запись.**

Примечание.

Никогда не используйте пароль, сходный с регистрационным именем. С точки зрения безопасности рекомендуется придумать пароль длиной не менее 10 символов и вручить его пользователю вместе с регистрационным именем в запечатанном конверте. Если вы создаете учетные записи заранее, то в течение нескольких дней до передачи пользователям конвертов с регистрационными данными целесообразно держать учетные записи отключенными.

Регистрационное имя пользователя должно устанавливаться внутренним предписанием компании так, чтобы в сети существовало единообразие. С расчетом на будущее развитие сети можно, например, определить, что регистрационное имя пользователя будет содержать первые три буквы его имени, две буквы фамилии и двузначный порядковый номер.

Примечание редактора.

Также можно рекомендовать использовать комбинацию из фамилии и инициалов, что-то вроде `vasiljev_ap`. Латинские символы дают широкие возможности для интерпретации русских букв и одну и ту же фамилию можно записать по-разному.

Создав запись по шаблону, откройте окно ее свойств и внесите необходимые изменения на вкладки **Адрес** и **Организация.** Одновременно про-

верьте, что разрешенное время регистрации соответствует служебному расписанию сотрудника.

Временная учетная запись для контрактника

Для этой записи не нужно шаблона, поскольку она всего одна. Ранее мы с вами договаривались, что на нашем предприятии время от времени работает один контрактник. И хотя их может быть и несколько (один сменяет другого), но единовременно на предприятии работает только один. А поскольку одновременно на предприятии может работать только один контрактник, то для них всех достаточно одной учетной записи и шаблон для нее не нужен.

А как же правило о недопустимости общей учетной записи для группы работников? А так: для каждого очередного контрактника меняйте пароль. Щелкните по учетной записи правой кнопкой мыши и из контекстного меню выберите команду **Смена пароля**. Введите и подтвердите первоначальный пароль и установите флажок **Требовать смену пароля при следующем входе в систему.**

Поскольку контрактник работает на предприятии временно, на вкладке **Учетная запись** установите срок окончания действия учетной записи, по истечении которого она окажется отключенной.

Примечание.

В целях безопасности отключать учетную запись рекомендуется и при уходе сотрудника в очередной отпуск.
В различных операционных системах семейства Windows 2000 названия некоторых команд могут различаться.

9.2.4. Учетные записи Администратор и Гость

Каждый пользователь, который хотя бы немного разбирается в операционных системах семейства Windows NT, знает, что стандартно они содержат встроенные учетные записи **Администратор** и **Гость**. Для входа под этими учетными записями необходимо узнать пароль, а регистрационное имя уже известно.

Под гостевой учетной записью много вреда причинить нельзя, потому что эта запись сильно ограничена в правах, но под именем Администратор домена пользователь имеет право делать в домене все, что хочет. Возможность регистрации постороннего под этими именами необходимо предотвратить. Решение заключается в том, чтобы переименовать учетную запись Администратор, а запись Гость вообще отключить.

Гостевую учетную запись рекомендуется использовать только в таких системах, которые не требуют почти никакой безопасности данных.

Переименование записи Администратор

Придумайте имя, которое трудно угадать (что-нибудь вроде `4ndr3j`). Далее поступайте следующим образом:

1. В консоли **Active Directory — Пользователи и компьютеры** раскройте папку Пользователи (Users) и затем в правом окне правой кнопкой мыши щелкните по записи Администратор.
2. Из контекстного меню выберите команду **Переименовать** и введите новое имя. Если появится предупреждение о необходимости выйти из системы, а затем снова войти, продолжите нажатием на кнопку **Да.** Отобразится диалоговое окно **Переименовать пользователя,** в котором в поле **Имя и фамилия** будет отображено заданное имя. Заполните остальные поля так, как показано на рис. 9.3.

Переименование записи Гость

Несмотря на то, что эта запись в большинстве систем отключена, несомненно, стоит переименовать и ее. Действуйте так же, как при переименовании записи Администратор. В этой книге мы выбрали в качестве нового имени `gh0$t`.

Для переименования этих двух записей в ОС Windows Server 2003 и Windows 2000 Server предусмотрены более эффективные возможности. Сейчас мы переименовали только доменные учетные записи Администратор и Гость, а их локальные тезки, существующие на каждом компьютере

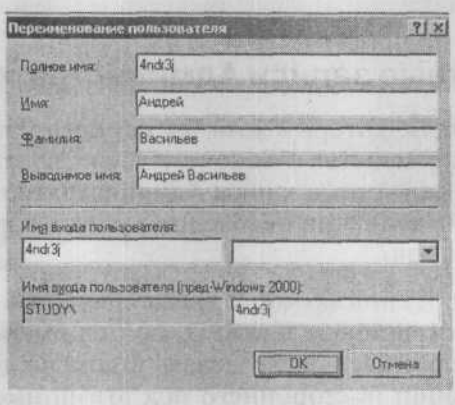


Рис. 9.3. *Переименование записи Администратор*

сети, остались без изменения. Переименовывать их вручную слишком долго. Другие возможности мы рассмотрим в главе 22, посвященной безопасности сервера и сети.

9.2.5. Членство в группах

Каждая вновь созданная учетная запись по умолчанию становится членом группы `Domain Users`. На каждой рабочей станции члены этой группы одновременно являются членами локальной группы `Users`, то есть получают обычные права доступа к ресурсам этого компьютера.

С членством в группе `Domain Users` манипулировать незачем. Может понадобиться разве что включение некоторых ее членов в другие группы. Дальнейшие сведения о работе с группами вы найдете в 11 главе.

9.2.6. Безопасность учетных записей

Учетная запись защищена своим паролем. Но чем может помочь пароль, даже самый длинный и сложный, если его разгласить или перехватить во время передачи по сети? Чтобы предотвратить злоупотребления такого рода, администратор должен заставить пользователей регулярно менять свои пароли.

Однако длинные пароли тоже не совсем бесполезны. Если пользователю придет в голову задать пароль, состоящий из двух символов, то такой пароль можно быстро подобрать простым перебором. Поэтому администратору следует требовать от пользователей придумывать себе длинные пароли (рекомендуется не короче 8 символов). Чтобы исключить использование в качестве пароля дат, номеров телефонов, имен и словарных слов, нужно требовать, чтобы пароль был сложным, то есть содержал заглавные буквы вперемешку со строчными, цифрами и знаками препинания. Такие пароли угадать или подобрать для злоумышленника намного труднее.

Среди других требований безопасности можно перечислить запрет повторно использовать пароль, который пользователь уже когда-то выбирал, или предписание не менять пароль в течение нескольких дней.

Все эти требования администратор может предъявить автоматически, настроив соответствующим образом политику безопасности. Дальнейшие сведения о принципах безопасности паролей вы найдете в 22 главе.

9.3. Создание учетной записи из командной строки

ОС Windows Server 2003 предоставляет еще один способ создания доменной учетной записи: команду **dsadd user**. При этом создание учетной записи с регистрационным именем `petrov` в контейнере `Users` домена `study.local` и предписанием сменить пароль после первого входа будет выглядеть следующим образом:

```
dsadd user DN=petrov, CN=Users, DC=study, DC=local,
-upn petrov@study.local -mustchpwd Yes
```

Созданная таким образом учетная запись по умолчанию отключена, что с точки зрения безопасности системы является нормой. Пароля у нее пока нет.

Примечание.

Утилита DSADD умеет создавать в активном каталоге и объекты других типов. Чтобы получить справку о ее возможностях, введите в командной строке **dsadd /?**. Чтобы узнать подробнее о создании при помощи этой утилиты учетных записей пользователей, введите **dsadd user /?**.

9.4. Куда исчезли локальные учетные записи?

Если клиентский компьютер является членом домена, на нем можно зарегистрироваться либо под доменной учетной записью, либо под локальной. Вторая возможность в доменах обычно не применяется, потому что создание локальных учетных записей для большого числа пользователей слишком трудоемко. Однако локальная учетная запись может понадобиться для решения какой-нибудь нестандартной задачи.

Чтобы зарегистрироваться на рабочей станции по локальной учетной записи, нужно в диалоге регистрации выбрать из выпадающего списка **Войти в** опцию **Имя компьютера (локальный компьютер)**. Вы зарегистрируетесь только на локальном компьютере, не входя в домен.

Рассмотрим сервер SRVR001. Здесь в списке **Войти в** присутствует только одна опция — STUDY (название домена). Это значит, что в компьютере SRVR001 нет ни одной локальной записи и для входа необходимо использовать только доменную учетную запись.

Для контроллеров домена под управлением Windows 2000 и Windows Server 2003 это нормальное явление. Как только рядовой сервер повышается в роли до контроллера домена, все локальные учетные записи пользователей и групп, существовавшие на нем, отключаются. Исключением является только первый контроллер домена, у которого все локальные учетные записи преобразуются в доменные. Пока сервер служит контроллером домена, на нем невозможно создать новые локальные учетные записи.

Подтверждение вышесказанного мы можем увидеть непосредственно на примере:

1. Зарегистрируйтесь на SRVR001 как администратор (не Администратор: вы уже переименовали эту учетную запись).
2. Откройте консоль **Администрирование → Управление компьютером.**
3. Хорошо рассмотрите левую часть окна консоли. Вы не увидите значка **Локальные пользователи и группы**, который присутствует на этом месте у рядовых серверов.

Примечание.

На контроллере домена под управлением ОС Windows 2000 папка **Локальные пользователи и группы** присутствует, но отмечена красным крестиком, так что открыть ее невозможно.

Положение, когда на контроллере домена нет даже локальной группы, является новым по сравнению с контроллером домена Windows NT 4.0.

Одно исключение все же существует в контроллере домена системы Windows Server 2000 или более поздних. Речь идет о локальной записи пользователя Администратор, при помощи которого на сервере можно зарегистрироваться только в режиме обновления службы каталога. Пароль этой учетной записи задается в ходе повышения роли сервера до контроллера домена, и его необходимо надежно хранить.

Чтобы сменить этот пароль впоследствии, на контроллере домена под управлением Windows 2000 поступайте следующим образом:

1. Перезагрузите сервер, во время загрузки нажмите клавишу F8 и выберите режим восстановления службы каталогов (Directory Services Restore Mode). Этим вы обеспечите то, что служба Active Directory не запустится.
2. Зарегистрируйтесь под учетной записью Администратор. Нажмите комбинацию клавиш Ctrl+Alt+Del и затем нажмите кнопку **Изменить пароль.**
3. Введите действующий и новый пароль.
4. Перезагрузите сервер.

На контроллере домена под управлением Windows Server 2003 вы можете изменить пароль для записи Администратор для восстановления службы каталогов еще проще:

1. Зарегистрируйтесь как администратор домена и откройте окно командной строки.
2. Введите команду **ntdsutil**.
3. Введите команду **reset dsrm password.**
4. После ответа «Создать новый пароль администратора для режима восстановления службы каталогов:» введите команду **reset password on server «имя сервера».**
5. После ответа «Введите пароль для записи администратора режима восстановления службы каталогов:» введите и подтвердите новый пароль.

Если подтверждение пароля прошло успешно, появится сообщение: «Пароль успешно установлен». Перезагружать сервер не нужно.

Пароль для режима восстановления службы каталогов можно изменить и на удаленном контроллере домена, если тот работает под управлением Windows Server 2003. Для этого служит команда **reset password on server work.study.com**. Удаленный сервер при этом должен работать в нормальном режиме (а не в режиме восстановления службы каталогов)

Если вы забыли пароль локального администратора контроллера домена, то не сможете восстановить службу каталога. Пароль можно восстановить, если в домене больше одного контроллера. Поступайте следующим образом:

1. Зарегистрируйтесь на том контроллере, пароль для восстановления которого утерян, как администратор домена и откройте окно командной строки.
2. Введите команду **dcpromo** и понизьте роль с контроллера домена до рядового сервера. После этого потребуется перезагрузить компьютер.
3. Снова зарегистрируйтесь и введите ту же команду **dcpromo**, чтобы снова установить контроллер домена. В ходе установки введите пароль для восстановления службы каталогов, который на сей раз запомните надежно.

9.5. Итоги

Для каждого пользователя домена заводится собственная доменная учетная запись. Под ней можно регистрироваться на любом компьютере домена за исключением контроллеров домена.

Создание нескольких учетных записей можно облегчить, создавая их на основе заранее заготовленного шаблона. Следует устанавливать для создаваемых учетных записей длинные и сложные пароли и требовать смены пароля пользователем при первом входе.

У каждого пользователя должна быть индивидуальная учетная запись. Общую учетную запись можно использовать как исключение, для временных работников предприятия. Для временных учетных записей необходимо настроить срок действия, по истечении которого запись будет автоматически отключена.

Если вам нужно создать сразу много записей, в домене Active Directory системы Windows Server 2003 вы можете использовать утилиту командной строки DSADD. Эта команда предназначена для управления не только пользовательскими учетными записями, но и объектами других типов.

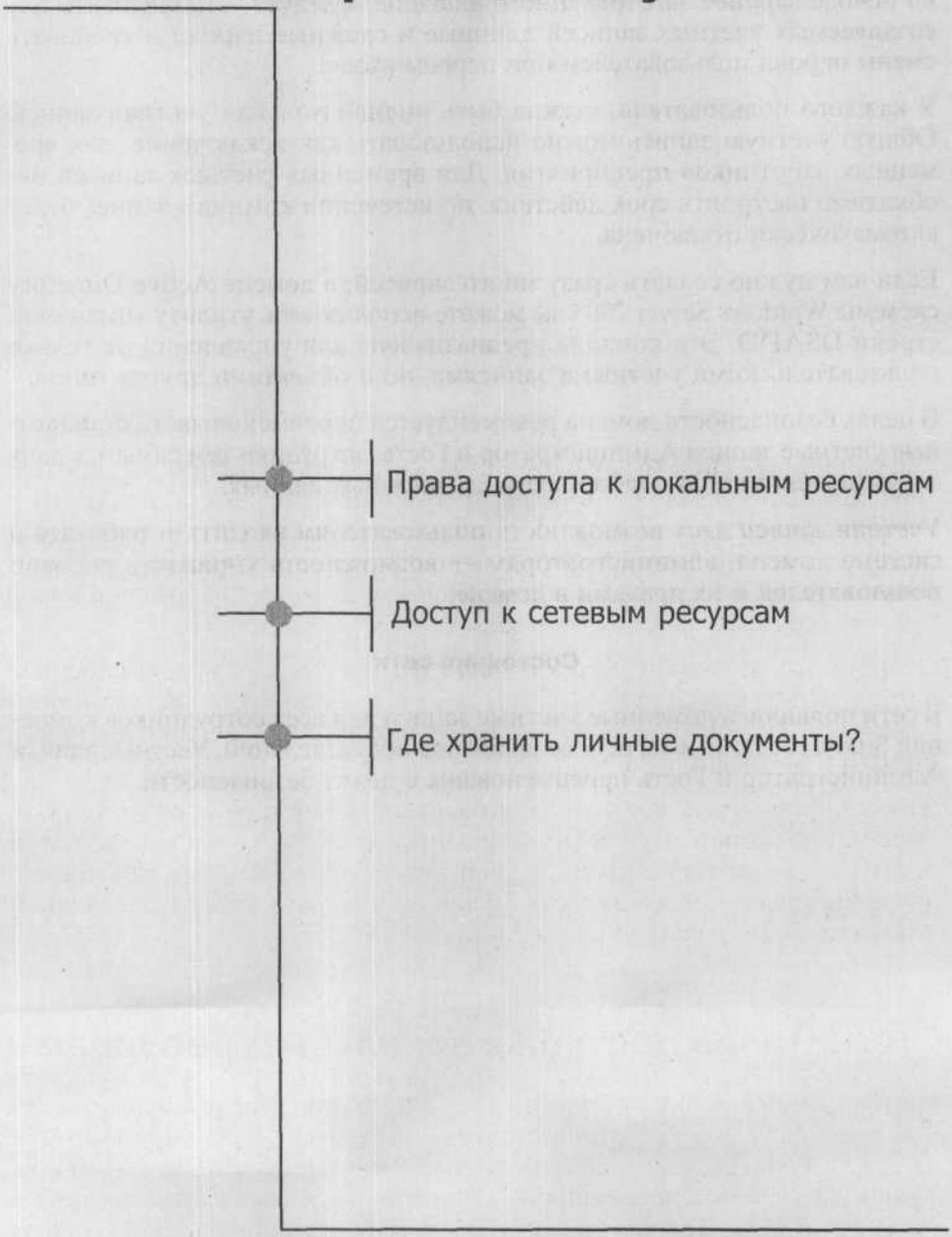
В целях безопасности домена рекомендуется переименовывать стандартные учетные записи Администратор и Гость, затрудняя тем самым задачу злоумышленника по подбору регистрационных данных.

Учетная запись дает возможность пользователям входить и работать в системе домена, администраторам — возможность управлять работой пользователей и их правами в домене.

Состояние сети

В сети появились доменные учетные записи для всех сотрудников компании Study, созданные на основе шаблонов подразделений. Учетные записи Администратор и Гость переименованы в целях безопасности.

Глава 10 Права доступа



Операционные системы Windows 2000/XP/2003 — это системы, предназначенные для установки в сетях, требующих надежности, быстроты и особенно безопасности. Организации, использующие эти системы, хотят обладать всей информацией и контролировать положение: кто имеет право входить в их сеть, с какими данными он может работать и какой уровень доступа к данным он имеет.

Обычно это не значит, что каждый пользователь, который способен подключиться к сети организации, автоматически имеет доступ ко всем данным. И внутри организации необходимо различать права доступа и иметь о нем представление.

Чтобы пользователь мог подключиться к сети, ему требуется знать регистрационное имя и пароль учетной записи. Потом, чтобы иметь доступ к документам, которые представляют интерес для него, ему необходимо нечто большее — право доступа к файлам. Эта глава является введением в типы прав доступа и способы работы с ними.

10.1. Права доступа к локальным ресурсам

Учетная запись пользователя имеет две функции. Первая, которую мы уже разобрали в достаточной степени, это возможность зарегистрироваться на локальном компьютере или в домене. Другой, не менее важной, функцией является возможность регулировать уровень прав доступа к объектам в сети. Такими объектами могут быть принтер, файл, папка, учетная запись и т.д.

Если вы хотите иметь доступ к объектам типа файл или папка, эти объекты должны быть расположены на разделе, отформатированном файловой системой NTFS.

Управление доступом к ресурсам очень важно для безопасности сети. Достаточно незначительной ошибки, опечатки или просто незнания, и важный документ сможет прочесть каждый пользователь, в худшем случае вы выясните, что его кто-то удалил. В такой ситуации необходимо иметь настроенный и функционирующий аудит, чтобы вы могли затем вычислить пользователя, который произвел эту операцию.

Дальнейшие сведения об аудите вы найдете в главе 22, посвященной безопасности сервера и сети.

10.1.1. Доступ к файлам. Разрешения NTFS

Разрешения NTFS и их проверка

Разрешения NTFS служат для регулирования прав доступа к объектам в разделах, форматированных в системе NTFS. Эти разрешения имеют смысл только в тех операционных системах, которые имеют возможность создавать эту файловую систему.

Разрешения NTFS можно задать на уровне папки или отдельных файлов. В ОС Windows разрешения по умолчанию наследуются от родительской папки, то есть разрешения, установленные для папки, действуют и на содержащиеся в ней файлы. Проверить это можно следующим образом:

1. Зарегистрируйтесь на PC001 как администратор домена.
2. Воспользуйтесь Проводником и в разделе C: создайте папку с названием «Договоры». В ней создайте два текстовых файла: `dogovor1.txt` и `dogovor2.txt` (файлы могут быть пустыми).
3. Щелкните правой кнопкой мыши по папке «Договоры» и из контекстного меню выберите команду **Свойства.**
4. В диалоговом окне свойств перейдите на вкладку **Безопасность.**
5. В верхней части окна отметьте группу **USERS (PC001\Users)** и нажмите кнопку **Удалить.** Появится сообщение, что эту группу удалить нельзя, так как разрешения унаследованы от родительской папки.
6. Нажмите кнопку **Дополнительно.**
7. В диалоговом окне **Дополнительные параметры безопасности** снимите флажок **Наследовать от родительского объекта**, после этого нажмите кнопку **Удалить** и закройте это окно нажатием кнопки **OK.**

8. Отобразится сообщение, что вы отказали всем пользователям в доступе к объекту **Договоры** с вопросом, хотите ли вы продолжить. Ответьте **Да.**
9. Теперь разрешим доступ к папке «Договоры» группе локальных администраторов и одному из рядовых пользователей — `Shop1`. Локальные администраторы должны иметь полный доступ ко всем ресурсам данного компьютера на тот случай, если он будет отключен от домена. При нормальной работе в домене управлять доступом к локальным ресурсам имеет право член группы администраторов домена, которая всегда входит в группу локальных администраторов. Нажмите кнопку **Добавить**. Отобразится диалоговое окно Выбора пользователя или группы. Если в поле **В следующем месте** отображено название DNS домена (`study.local`), нажмите на кнопку **Размещение** и выберите размещение PC001.
10. В поле **Введите имена выбираемых объектов** укажите группу **Administrators** и нажмите кнопку **Проверить имена.** Если все правильно, введенный текст должен измениться на имя **PC001\Administrators.** Затем нажмите кнопку **OK.**
11. На вкладке **Безопасность** в области **Разрешения** для группы локальных администраторов установите флажок **Разрешить/Полный доступ.**
12. Снова нажмите кнопку **Добавить** и в окне выбора пользователей измените **Размещение** на домен `study.local`, а в поле **Введите имена выбираемых объектов** укажите имя `Shop1`. Нажмите кнопку **Проверить имена.**
13. Нажмите **OK** и рассмотрите разрешения, выданные рядовому пользователю по умолчанию. В столбце **Разрешить** установите флажок **Запись** и нажмите кнопку **OK.**

Разрешения, предоставленные пользователю `Shop1` на папку «Договоры», действительны и для ее дочерних объектов. Чтобы убедиться в этом, закройте окно свойств папки и вызовите окно свойств файла `dogovor2.txt`. Удалить разрешения на этот файл вам не удастся, пока вы не снимете флажок **Наследовать от родительского объекта.**

Теперь нужно проверить назначенные права доступа. Пользователь `Shop1` имеет следующие права доступа к папке и к файлам: **Чтение, Чтение и выполнение** и **Запись.** Теперь пользователь способен открыть файл, просмотреть его содержание, при необходимости добавить изменения и добавить файл:

1. Зарегистрируйтесь на PC001 как пользователь `Shop1`.
2. Перейдите в папку «Договоры» и откройте файл `dogovor1.txt`. Запишите в него что-нибудь и сохраните файл.

3. Теперь попробуйте удалить файл `dogovor2.txt`. Эта попытка будет безуспешной, так как у вас нет разрешения на удаление. Поэтому отобразится сообщение об ошибке.

Описание отдельных прав доступа NTFS

Мы кратко познакомились с основными разрешениями NTFS и с понятием наследования разрешений, которое в ОС Windows включено по умолчанию. Следующая таблица приводит значение отдельных прав доступа NTFS.

Стандартные разрешения NTFS для файлов и папок *Таблица 10.1*

Разрешение	Допускаемые действия	Примечание
Чтение	Разрешается чтение файла и просмотр его свойств: имени владельца, разрешений и атрибутов. Для папки разрешается просмотр вложенных файлов и подпапок	
Чтение и выполнение	То же, что «Чтение», плюс возможность запуска, если файл исполняемый. Для папки разрешается доступ к файлам в подпапках, даже если нет доступа к самой папке	
Просмотр содержимого папки	Разрешается просмотр списка файлов и подпапок	Доступно только в свойствах папки
Запись	Разрешается перезапись файла и изменение его атрибутов. Для папки разрешается добавление файлов и подпапок, а также изменение атрибутов папки	
Изменение	Разрешается все, что предусмотрено разрешениями «Запись» и «Чтение и выполнение» плюс удаление файла или папки	
Полный доступ	Разрешается все, в том числе возможность становиться владельцем файла или папки и заново назначать разрешения	
Особые разрешения	Задает набор специальных (нестандартных) разрешений	

Пользователю `Shop1` мы присвоили права доступа «Чтение», «Чтение и Выполнение», «Просмотр содержимого папки» и «Запись». При открытии папки использовалось право доступа «Просмотр содержимого папки», при открытии файла — «Чтение» и при сохранении — «Запись».

Право доступа «Запись» дает возможность создавать новые файлы. Проверьте это следующим образом: в папке «Договоры» создайте новый текстовый файл. Если вы попытаетесь изменить его название, отобразится сообщение об ошибке, означающее, что у вас недостаточно прав (разрешения «Изменить» у вас нет). Именем файла останется «Новый текстовый документ», присвоенное ему по умолчанию.

Особые разрешения NTFS

Что обозначает, например, разрешение «Чтение»? Достаточно ли этого разрешения для того, чтобы отобразить свойства файла и посмотреть, например, дату его создания и последних изменений? Какие права доступа необходимы для просмотра списка разрешений?

Если вы хотите знать ответы на эти вопросы, нужно посмотреть так называемые особые разрешения NTFS. Все стандартные разрешения, в том числе «Чтение», представляют собой совокупности особых разрешений. Чтобы увидеть эти разрешения, поступайте следующим образом:

1. Зарегистрируйтесь на PC001 как администратор.
2. Откройте окно свойств файла `dogovor1.txt` и выберите вкладку **Безопасность**. На ней отображены стандартные разрешения. Чтобы увидеть нестандартные, в верхней части окна выберите пользователя или группу, а затем нажмите кнопку **Дополнительно**.

Вы видите, что разрешение «Чтение» предполагает такие особые разрешения, как «Чтение атрибутов», дающее возможность просматривать свойства файла, и «Чтение разрешений», позволяющее просматривать список разрешений данного файла.

Иногда наличие этих разрешений нежелательно: например, может возникнуть необходимость запретить пользователю просматривать вкладку **Безопасность** в окне свойств файла. В таком случае вы можете установить флажок **Запретить** для соответствующего особого разрешения.

10.1.2. Владелец файла

Кто такой владелец файла и какими он обладает преимуществами?

Начнем с примера. Зарегистрируйтесь на PC001 как пользователь `Shop1` и попытайтесь переименовать файл «Новый текстовый документ», который вы создали в предыдущем параграфе. Вам это не удастся, потому что разрешения «Изменение» у вас нет.

Теперь откройте окно свойств этого файла и перейдите на вкладку **Безопасность**. Выберите пользователя `Shop1`, в поле **Разрешения** установите флажок **Разрешить/Изменить** и нажмите **OK**. После этого повторите попытку переименовать файл: на этот раз она должна оказаться успешной.

Попробуйте проделать то же самое с файлом `dogovor1.txt`, созданным от имени администратора. Оказывается, у вас недостаточно прав для изменения разрешений этого файла.

Дело в том, что среди всех субъектов доступа к файлам и папкам на файловой системе NTFS есть один особый — владелец файла. По умолчанию им становится тот, кто создал файл. Владелец имеет право делать со своим файлом все, что хочет, в том числе изменять разрешения на него для себя и для других пользователей. Возможно даже отказать в доступе к своему файлу членам группы администраторов.

Надолго ли можно уберечь таким образом свой файл от любопытства администратора? Нет, только до тех пор, пока администратор не «присвоит» его, назначив владельцем себя. Это делается так:

1. Под именем администратора откройте окно свойств файла, который раньше назывался «Новый текстовый документ», и перейдите на вкладку **Безопасность**.
2. Нажмите кнопку **Дополнительно** и в окне **Дополнительные параметры безопасности** перейдите на вкладку **Владелец**. В поле **Текущий владелец** вы увидите имя пользователя `Shop1`.
3. В поле **Изменить владельца на** выберите свою учетную запись или группу Администраторы и нажмите кнопку **OK** два раза.
4. На вкладке **Безопасность** добавьте к списку пользователей и групп, для которых установлены разрешения, группу администраторов и установите для нее разрешение «Полный доступ». У пользователя `Shop1` полный доступ отберите и оставьте, например, только «Чтение».

Кто может стать владельцем

Как мы только что показали, право собственности на файл предоставляет неограниченные права доступа к нему. С точки зрения администратора домена очень важно знать, кто может стать владельцем файла и какое для этого потребуется право доступа.

- Первоначально владельцем файла становится пользователь, создавший этот файл.
- Впоследствии владельцем может стать тот, кто получил право собственности. Право стать владельцем файла по умолчанию принадлежит:
  - тем, у кого на этот файл есть стандартное разрешение «Полный доступ» или специальное разрешение «Стать владельцем»;
  - членам группы администраторов.

Примечание.

Разрешение становиться владельцем файлов настраивается в политиках безопасности локального компьютера или домена.

В ОС Windows XP Professional и более ранних нельзя назначить владельцем файла не себя, а другого пользователя: можно только предоставить ему разрешение стать владельцем. В Windows Server 2003 право собственности передать другому можно.

10.1.3. Разрешения следует назначать очень аккуратно

Правильное понимание настройки разрешений, особенно в связи с явлением наследования, требует некоторого времени обучения и особенно практики. Приведем пример, который покажет, что не все так просто, как кажется на первый взгляд.

Верните пользователю `Shop1` разрешение «Полный доступ» на папку «Договоры» и запретите ему доступ к файлу `dogovor1.txt` (сняв предварительно флажок **Наследовать от родительского объекта** в диалоге **Дополнительные параметры безопасности** свойств этого файла).

Зарегистрируйтесь на PC001 под именем `Shop1` и откройте папку «Договоры». Вы не сможете ни прочитать файл `dogovor1.txt`, ни изменить его разрешения, добавив себе прав. Зато вы сможете удалить этот файл.

Возможно, для вас это удивительно, потому что до сих пор вы предполагали, что разрешения на уровне файла имеют приоритет над разрешениями на родительскую папку. Но это не так. Перерегистрируйтесь как администратор и просмотрите специальные разрешения на папку «Договоры» пользователя `Shop1`. Вы видите, что разрешение «Удаление подпапок и файлов» у него есть.

Именно поэтому стоит семь раз отмерить, прежде чем один раз отрезать. Следует тщательно проверить задуманную конфигурацию разрешений до того, как вы введете ее в систему.

10.2. Доступ к сетевым ресурсам

Если пользователю нужен доступ к файлам в папках на удаленном компьютере, эти папки должны быть разделяемыми. Доступ к разделяемой папке можно ограничить. Если папка, к которой предоставлен доступ по сети, расположена на файловой системе NTFS, то она и ее содержимое защищены еще и разрешениями NTFS. В этом параграфе мы рассмотрим, как взаимодействуют права доступа по сети с разрешениями NTFS.

10.2.1. Открытие сетевого доступа к папке

Чтобы превратить локальную папку в сетевой ресурс, первым делом нужно сделать ее разделяемой, то есть открыть доступ к ней по сети. В ОС Windows 2000 и новее сделать это имеет право член группы администраторов, а в домене — член группы операторов сервера.

Сделать локальную папку разделяемой можно либо средствами Проводника Windows, либо из консоли **Администрирование → Управление компьютером** (объект **Общие папки**). Только вторым из этих способов можно сделать общей удаленную папку.

На вкладке **Доступ** в диалоговом окне свойств папки, которую вы хотите сделать общей, есть кнопка **Разрешения**. Она служит для того, чтобы ограничить доступ к разделяемой папке для отдельных пользователей или групп. По умолчанию в ОС Windows Server 2003 группе «Все» предоставляется право «Только чтение», а в Windows 2000/XP — «Полный доступ». Это значит, в Windows 2000/XP настройку по умолчанию оставлять небезопасно.

10.2.2. Взаимодействие прав доступа

Если общая папка находится в разделе с файловой системой NTFS, для нее установлены собственные разрешения. Если пользователь обращается к этой папке локально (сидя за тем же компьютером, на диске которого она расположена), то для него действуют только эти разрешения.

Если он обращается к папке по сети, то разрешения NTFS взаимодействуют с разрешениями на доступ к общему ресурсу так, как показано в таблице 10.2 (в этом примере пользователь `Shop1` не входит в группу администраторов).

Результат взаимодействия прав доступа для пользователя Shop1 *Таблица 10.2*

Разрешения NTFS	Право доступа к общей папке	Результат
Shop1 — «Чтение»	«Все» — «Чтение»	«Чтение»
Shop1 — «Полный доступ»	Администраторы — «Полный доступ»	нет доступа
Shop1 — «Чтение», «Запись»	«Все» — «Чтение»	«Чтение»
Shop1 — «Чтение»	«Все» — «Полный доступ»	«Чтение»
Shop1 — «Полный доступ»	«Все» — «Чтение»	«Чтение»

Из последнего примера видно, что пользователь Shop1 сможет воспользоваться своим разрешением NTFS на полный доступ к папке, только если зарегистрируется непосредственно на сервере, на жестком диске которого расположена эта папка. По сети он получит доступ только на чтение.

Практическое применение разрешений NTFS и прав доступа к общим ресурсам мы покажем в главе 12.

10.3. Где хранить личные документы?

С точки зрения каждого пользователя, именно личные документы должны иметь наивысшую степень безопасности. Поэтому обычно пользователь хочет, чтобы к его документам не имел доступа никто, включая администраторов.

Этого можно добиться правильной настройкой разрешений, но традиционно рядовой пользователь не имеет права манипулировать разрешениями, за исключением тех файлов и папок, для которых он является владельцем. Поэтому пользователям приходится полагаться на администратора, а администраторы, в свою очередь, должны хорошо знать все возможности, которые они могут предложить пользователям.

Не говоря уже о безопасности данных в смысле их регулярного резервного копирования, самым надежным местом для хранения личных документов в ОС Windows 2000/XP является папка «Мои документы» (%system-drive%\Documents and Setting\%username%). Она составляет часть профиля пользователя, и операционная система клиентского компьютера сама заботится о том, чтобы разрешать доступ к данным в этой папке только данному пользователю. Посторонним запрещен доступ как к чужому профилю, так и ко всем его подпапкам.

Клиентская операционная система устанавливает разрешение «Полный доступ» для того пользователя, которому принадлежит профиль, группы локальных администраторов и группы SYSTEM (встроенная системная группа). Пользователь имеет возможность запретить доступ администраторам, но мало кто пользуется этой возможностью. Во-первых, пользователи о ней обычно не знают, а во-вторых, администратор всегда может вернуть себе право доступа.

Настоятельно рекомендуется хранить личные документы только в папке «Мои документы». Если к некоторым документам должны иметь доступ несколько сотрудников, то для таких файлов следует создать отдельную сетевую папку, настроив права доступа к ней вручную.

10.4. Итоги

В разделах, отформатированных файловой системой NTFS, можно ограничить доступ к файлам и папкам для отдельных пользователей или групп при помощи разрешений NTFS.

Существует пять стандартных разрешений NTFS для файлов и шесть для папок (шестое — разрешение «Просмотр содержимого папки»). Каждое стандартное разрешение складывается из нескольких специальных разрешений.

Неограниченное право доступа к файлу (папке) имеет его владелец. Первоначально владельцем становится пользователь, который создал данный файл. Он имеет возможность изменять разрешения на этот файл для себя и для других. Новым владельцем файла может стать либо тот пользователь, которому предыдущий владелец предоставил такое разрешение, либо член группы локальных администраторов. В ОС Windows Server 2003 владелец может передать право собственности на файл другому пользователю.

По умолчанию разрешения наследуются от родительской папки. Если вы хотите изменить разрешения на файл, то первым делом нужно отменить наследование для этого файла.

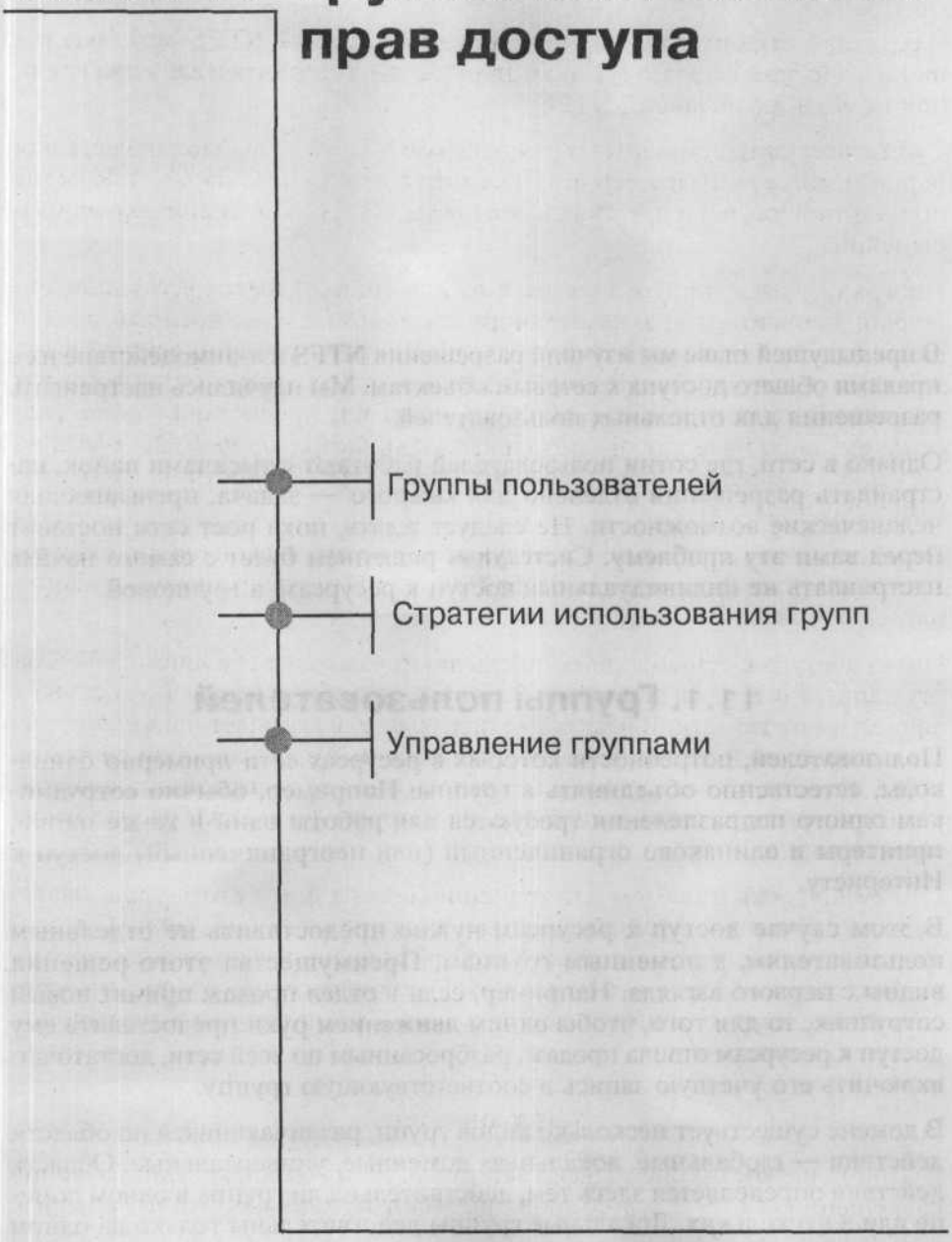
Права доступа к сетевой папке определяются как разрешениями NTFS на эту папку, так и разрешениями, установленными при открытии доступа к данной папке по сети. В результате пользователь получает наименьшее из этих разрешений. Если права, предоставленные ему файловой системой NTFS, больше, то воспользоваться ими он сможет только тогда, когда зарегистрируется на том компьютере, на котором физически расположена сетевая папка.

Самым надежным местом для хранения личных документов пользователя является папка «Мои документы», входящая в его профиль. С точки зрения администратора домена такое размещение оптимально, потому что все папки «Мои документы» можно разместить на сервере, что обеспечит как доступ к ним с любой рабочей станции, так и регулярное резервное копирование.

Состояние сети

В этой главе состояние нашей сети никак не изменилось. Для изучения разрешений NTFS были созданы временные папки и файлы, которые теперь вы можете удалить.

Глава 11 Группы как шаблоны прав доступа



В предыдущей главе мы изучили разрешения NTFS и взаимодействие их с правами общего доступа к сетевым объектам. Мы научились настраивать разрешения для отдельных пользователей.

Однако в сети, где сотни пользователей работают с тысячами папок, настраивать разрешения отдельно для каждого — задача, превышающая человеческие возможности. Не следует ждать, пока рост сети поставит перед вами эту проблему. Системным решением будет с самого начала настраивать не индивидуальный доступ к ресурсам, а групповой.

11.1. Группы пользователей

Пользователей, потребности которых в ресурсах сети примерно одинаковы, естественно объединять в группы. Например, обычно сотрудникам одного подразделения требуются для работы одни и те же папки, принтеры и одинаково ограниченный (или неограниченный) доступ к Интернету.

В этом случае доступ к ресурсам нужно предоставить не отдельным пользователям, а доменным группам. Преимущества этого решения видны с первого взгляда. Например, если в отдел продаж принят новый сотрудник, то для того, чтобы одним движением руки предоставить ему доступ к ресурсам отдела продаж, разбросанным по всей сети, достаточно включить его учетную запись в соответствующую группу.

В домене существует несколько видов групп, различающихся по области действия — глобальные, локальные, доменные, универсальные. Область действия определяется здесь тем, действительна ли группа в одном домене или в нескольких. Локальные группы действительны только на одном компьютере и в домене используются редко, потому что ими нельзя управлять централизованно.

11.1.1. Типы групп в домене Active Directory

В домене Active Directory можно встретить следующие типы групп:

- **Группы безопасности.** Это те группы, для которых можно назначать права и разрешения. Права определяют, какая деятельность разрешается в домене члену подобной группы (пользователю или компьютеру), а разрешения определяют, к каким объектам в сети они будут иметь доступ. Группы безопасности можно использовать и для рассылки e-mail сообщений многим пользователям. Сообщение отсылается лишь один раз, но при этом его получают все члены группы. Для этого, впрочем, в сети должен быть установлен продукт Microsoft Exchange Server 2003. В этом случае группы безопасности ведут себя так же, как группы распространения.
- **Группы распространения.** Эти группы предназначены только для рассылки пользователям сообщений электронной почты. Для них не определяются права доступа к сетевым объектам.

Примечание.

Группы безопасности имеют все свойства групп распространения, но не наоборот. Тогда зачем вообще нужны группы распространения? Дело в том, что некоторые приложения могут работают только с ними, а не с группами безопасности.

11.1.2. Режим работы домена

Описание режимов работы домена

В качестве начала разъяснений в данной области приведём краткий пример.

1. Зарегистрируйтесь на SRVR001 как Администратор.
2. Запустите консоль **Active Directory — пользователи и компьютеры** и в папке **Users** попытайтесь создать новую группу. Появится диалоговое окно, изображённое на рис. 11.1.
3. Обратите внимание, что переключатель **Область действия группы** нельзя установить в положение **Универсальная**.

Это зависит от режима работы домена. Существует три режима работы домена Active Directory в системе Windows Server 2003. Режим определяет, какие операционные системы можно установить на контроллерах домена, и в соответствии с этим ограничиваются и некоторые возможности.

Типы операционных систем и возможные в них группы пользователей отражает таблица 11.1.

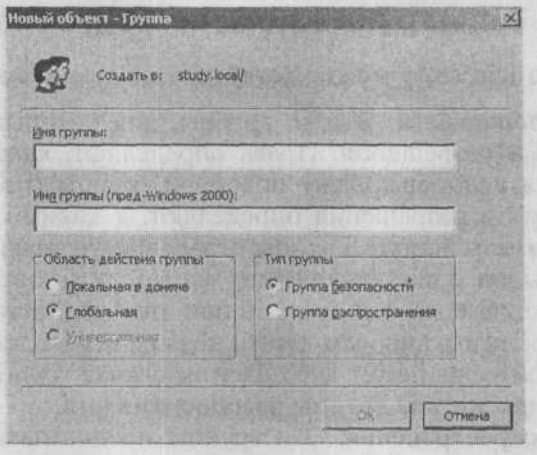


Рис. 11.1. *Создание новой группы*

Режимы работы домена *Таблица 11.1*

	Windows 2000 mixed (смешанный)	Windows 2000 native (основной)	Windows Server 2003
Возможные операционные системы на контроллерах домена	Windows NT 4.0 Server, Windows 2000, Windows Server 2003	Windows 2000, Windows Server 2003	Windows Server 2003
Возможные типы групп	Глобальные, локальные доменные	Глобальные, локальные доменные, универсальные	Глобальные, локальные доменные, универсальные

Объяснение приведённых ограничений в целом логично. Поскольку в режиме Windows 2000 mixed, например, могут работать и контроллеры домена с системой Windows NT 4.0 Server, в которых ещё не было понятия универсальной группы, этот тип групп использовать нельзя. Естественно, в данном режиме домена это не единственное ограничение.

Домен Active Directory с системой Windows Server 2003 по умолчанию устанавливается в режиме Windows 2000 mixed. Это означает, что в случае необходимости можно добавить контроллеры домена с системой Windows NT 4.0.

Уровень работы домена можно в любое время повысить, но вернуть обратно будет невозможно. Поэтому не следует менять режим без особых оснований.

Изменение режима работы домена в Windows Server 2003

Изменение режима работы домена в Windows Server 2003 производится следующим образом:

1. Зарегистрируйтесь на SRVR001 как Администратор.
2. Запустите консоль **Active Directory — пользователи и компьютеры.**
3. Щелкните правой кнопкой мыши по домену `study.local` и из контекстного меню выберите команду **Изменение режима работы домена.** Откроется диалоговое окно (рис. 11.2).

Изменение режима работы домена в Windows Server 2000

Изменение режима работы домена в Windows Server 2000 состоит из следующих этапов:

1. Зарегистрируйтесь на контроллере домена как Администратор.
2. Запустите консоль **Active Directory — пользователи и компьютеры.**
3. Щелкните правой кнопкой мыши по домену и из контекстного меню выберите команду **Изменение режима работы домена.** В диалоговом окне свойств будет отображён уровень. Если текущий режим — смешанный, то с помощью кнопки **Изменить** вы можете переключить домен в основной режим.

Разница в свойствах различных групп проявляется в сети с несколькими доменами. Поскольку никогда не известно заранее, не расширится ли однодоменная сеть, включив в себя ещё несколько доменов, следует хорошо разобраться в этих свойствах.

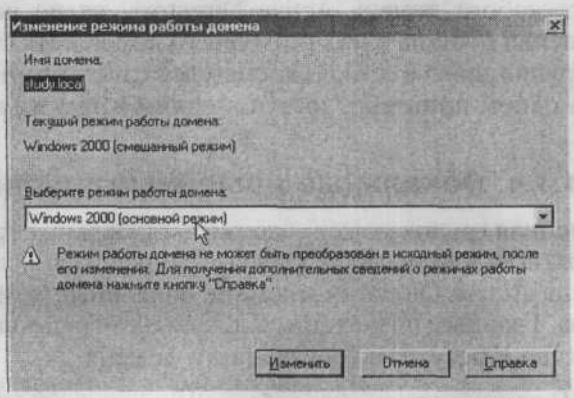


Рис. 11.2. *Изменение режима работы домена*

11.1.3. Глобальные группы

Глобальная группа может содержать учётные записи пользователей, компьютеров или групп, созданные в том же домене, на котором была создана и эта. Глобальным группам, хоть это и не рекомендуется в большинстве случаев, можно разрешать доступ и наделять правами в каком угодно домене в Active Directory (отсюда и её название — «глобальная»).

Свойства глобальных групп можно обобщить в следующих пунктах:

- **Членство.** В домене со смешанным режимом работы глобальная группа может содержать учётные записи пользователей и учётные записи компьютеров того же домена, что и она сама. В домене с режимом Windows 2000 native или Windows Server 2003 глобальная группа может содержать не только учётные записи пользователей и компьютеров, но и записи глобальных групп, опять же размещённых на том же самом домене.
- **Группа может быть членом.** В домене со смешанным режимом работы она может быть членом только локальных доменных групп. В домене с режимом Windows 2000 native или Windows Server 2003 она может быть членом локальных доменных и универсальных групп любого домена Active Directory и членом глобальных групп любого домена (не обязательно домена Active Directory).
- **Область видимости группы.** Глобальная группа «видна» в собственном домене и во всех его доверенных доменах. Доверенными являются, в частности, другие домены одного и того же леса Active Directory.
- **Права доступа.** Глобальной группе могут быть назначены права доступа в любом домене Active Directory.
- **Применение глобальных групп.** Ввиду того, что глобальные группы видимы из любого домена Active Directory, их не используют для предоставления доступа к ресурсам своего домена. Их главной задачей является группировка в сети пользователей с похожими требованиями (печать на одном принтере, доступ к одним и тем же папкам и т.д.).

11.1.4. Локальные доменные группы

Локальная доменная группа может содержать глобальные группы, универсальные группы, пользовательские учётные записи и записи компьютеров с любого домена Active Directory и другие локальные доменные группы родного домена. Главным назначением локальных групп является предоставление доступа к ресурсам собственного домена.

- **Членство.** В домене с режимом работы Windows 2000 mixed локальная доменная группа может содержать учётные записи пользователей и глобальных групп с любого домена. При этом на рядовых серверах локальных доменных групп быть не может. В домене с режимом

Windows 2000 native или Windows Server 2003 локальная доменная группа может содержать учётные записи пользователей, глобальные группы и универсальные группы с любого домена Active Directory и локальные доменные группы с того же домена.

- **Группа может быть членом.** В домене с режимом работы Windows 2000 mixed локальная доменная группа не может быть членом какой-либо другой группы, а с режимом Windows 2000 native или Windows Server 2003 она может быть членом локальных доменных групп того же домена.
- **Область видимости группы.** Локальная доменная группа видна только в домене, в котором она была создана (отсюда название «локальная»).
- **Права доступа.** Локальной доменной группе могут быть назначены права доступа только в том домене, в котором она была создана.
- **Применение локальных доменных групп.** Локальные доменные группы предназначены для предоставления доступа к ресурсам того домена, в котором они были созданы.

11.1.5. Универсальные группы

Универсальные группы могут содержать учётные записи пользователей, компьютеров или групп из любого домена Active Directory. Универсальным группам безопасности можно разрешать доступ к ресурсам любого домена Active Directory. Свойства универсальных групп можно охарактеризовать в следующих пунктах:

- **Членство.** В домене с режимом работы Windows 2000 mixed нельзя создавать универсальные группы. В домене с режимом работы Windows 2000 native или Windows Server 2003 универсальная группа может содержать учётные записи пользователей, компьютеров, глобальные группы или универсальные группы с любого домена Active Directory.
- **Группа может быть членом.** В домене с режимом Windows 2000 native или Windows Server 2003 данная группа может быть членом локальных доменных групп и универсальных групп любого домена.
- **Область видимости группы.** Универсальная группа видна из любого домена Active Directory.
- **Права доступа.** Универсальной группе могут быть назначены права доступа в любом домене Active Directory.
- **Применение универсальных групп.** Универсальные группы предназначены для объединения глобальных групп и облегчения доступа к объектам нескольких доменов Active Directory. Учитывая сравнительную простоту нашей сети, в универсальных группах нет необходимости, поэтому пока что нет необходимости и повышать режим работы домена.

11.2. Стратегии использования групп

Наверное, от всех этих перечислений, какая группа может входить в состав другой группы и каковы возможные варианты доступа к объектам доменов, у вас в голове некоторый туман. Непонимание этого может привести ко всё возрастающему хаосу в домене.

Поэтому неплохо ознакомится со следующими стратегиями использования групп. Эти стратегии разработаны для того, чтобы по возможности облегчить работу администраторов, и чтобы при этом вся конфигурация получилась как можно более простой и понятной.

11.2.1. Обозначения

Для единообразия будем следовать обозначениям объектов, принятым в англоязычной литературе:

- **A** учётные записи пользователей (user **A**ccounts).
- **G** глобальные группы (**G**lobal groups).
- **DL** локальные доменные группы (**D**omain **L**ocal groups).
- **U** универсальные группы (**U**niversal groups).
- **P** право доступа (**P**ermission).

11.2.2. Самая распространенная стратегия (стратегия A G DL P)

Эту стратегию можно обозначить как A G DL P. Это означает, что учётные записи пользователей являются членами глобальной группы, а для локальной доменной группы настроены права доступа к ресурсу (например, к папке с файлами). Чтобы пользователи получили доступ к этому ресурсу, остаётся сделать только одно — включить глобальную группу в локальную доменную группу.

Весь этот процесс можно проще изобразить следующим образом:

$$A \rightarrow G \rightarrow DL \leftarrow P$$

Для примера используем эту стратегию в нашем домене study.local. Пусть пользователям из торгового отдела требуется доступ к папке «Договоры». Если мы будем придерживаться правила, что разрешение на доступ даётся не отдельными пользователям, а только группам, то порядок наших действий будет таким:

1. Создание глобальной группы безопасности.
2. Включение учётных записей продавцов в эту группу.
3. Создание локальной доменной группы безопасности.

4. Настройка разрешений на доступ к папке «Договоры» для этой локальной группы.
5. Включение глобальной группы в локальную доменную группу.

Может показаться, что проще было бы провести конфигурацию иначе, например, что локальная доменная группа в этой структуре не нужна. Рассмотрим три наиболее частых заблуждения.

МНЕНИЕ 1: ГРУППЫ НЕ НУЖНЫ, СЛЕДУЕТ ПРЯМО РАЗРЕШИТЬ ДОСТУП ПОЛЬЗОВАТЕЛЯМ ЧЕРЕЗ ИХ УЧЕТНЫЕ ЗАПИСИ. Как было сказано ранее, эту стратегию можно использовать только в очень небольших сетях, конфигурацию которых администратор постоянно держит в уме. Как только сеть достигнет определённой величины, это станет невозможно.

МНЕНИЕ 2: ЛОКАЛЬНАЯ ДОМЕННАЯ ГРУППА ЛИШНЯЯ, СЛЕДУЕТ ДАТЬ РАЗРЕШЕНИЕ НА ДОСТУП СРАЗУ ГЛОБАЛЬНОЙ ГРУППЕ. Речь идёт о возможности выбросить группу DL. Эту стратегию можно использовать только в небольших сетях, где заранее известно, что новых доменов Active Directory не появится.

Посмотрим, чем грозит такая стратегия, когда появляется новый домен. Пусть предприятие `Study` открыло филиал и создало для него ещё один домен (например, `eu.study.local`). Так же, как и в домене `study.local`, в домене `eu.study.local` будут находиться учётные записи продавцов, которым нужен доступ к папке «Договоры». Если объединить их в глобальную группу и предоставить доступ ей, то на вкладке **Безопасность** в свойствах папки «Договоры» появится второй субъект доступа — эта глобальная группа. Еще один домен — еще один субъект доступа и так далее, до полного хаоса и неуправляемости.

МНЕНИЕ 3: У МЕНЯ ВСЕГО ОДИН ПОЛЬЗОВАТЕЛЬ, КОТОРОМУ НУЖНО РАЗРЕШИТЬ ДОСТУП К КОНКРЕТНОЙ ПАПКЕ. СОЗДАВАТЬ РАДИ ЭТОГО ЕЩЁ ДВЕ ГРУППЫ НЕ ИМЕЕТ СМЫСЛА. Действительно, настроить разрешения для единственного пользователя значительно быстрее. Но что если пользователь с такими требованиями не останется единственным? Второго и третьего добавить вручную еще можно, но рано или поздно придется перестраивать всю схему безопасности данного ресурса, стараясь при этом не помешать работе уже существующих пользователей. Нет, если с самого начала поступать правильно, то потом работы будет существенно меньше.

11.2.3. Альтернативные стратегии

Стратегия A G P

Эта стратегия соответствует приведённому выше мнению 2. Стратегию **A → G ← P** рекомендуется использовать только в очень небольших сетях и только исходя из того, что в Active Directory никогда не будет более одного домена. В противном случае вся система рухнет.

Стратегия A G U DL P

В этой стратегии впервые будет применена универсальная группа. На первый взгляд универсальные группы кажутся очень удобными, поскольку у них есть масса преимуществ, но нет недостатков локальной и глобальной групп. Чаще всего они помогают упростить схему сети.

Сеть с одним доменом Active Directory, однако, никогда не является настолько сложной, чтобы обязательно было использовать этот тип групп. Универсальные группы устанавливаются там, где доменов несколько.

Однако по сравнению с доменной и глобальной группой универсальные группы отличаются по одному важному параметру, а именно — местом, в котором сосредоточена вся информация о том, кто является членом данной группы. В двух предыдущих типах групп сведения о членстве хранятся на всех контроллерах домена, в котором созданы группы, а членство в универсальной группе зарегистрировано на **серверах глобального каталога** леса Active Directory.

Если изменится состав, скажем, локальной доменной группы, сведения об изменении будут скопированы на все контроллеры домена. Если же произойдёт изменение состава универсальной группы, сведения об изменении будут распространяться среди серверов глобального каталога, которые могут находиться (как рекомендуется) в каждом домене. Таким образом, локальная сеть будет перегружена передачей данных между серверами глобального каталога, что отрицательно скажется на работе всех клиентов сети.

Универсальные группы именно поэтому используются нечасто, и только в случаях, когда действительно нужно упростить всю систему. В нашей однодоменной сети мы, естественно, с ними работать не будем.

Стратегия A G L P

Здесь L — это локальная группа, а не локальная доменная. Эта стратегия рекомендуется для доменов с системой Windows NT 4.0 Server, в которых локальных доменных групп не существует.

Слабые места этого решения в современном домене Active Directory очевидны. Локальными группами нельзя управлять централизованно. Чем больше таких групп, тем ближе сеть к хаосу. Другой недостаток локальных групп — невозможность получить через членство в них доступ к ресурсам на удаленном компьютере.

Если бы, например, у вас на одном компьютере была бы локальная группа с разрешением на доступ к папке «Договоры», а на другом компьютере находились бы остальные папки торгового отдела, вам пришлось бы создать ещё одну локальную группу (на втором компьютере) и настроить разрешения для нее. По сравнению со стратегией A G DL P, где вам не нужно создавать ещё одну дополнительную группу, здесь необходимо выполнить больший объём работ.

11.3. Управление группами

Предположим, что далее мы в нашей сети будем руководствоваться стратегией A → G → DL ← P, тогда начинает вырисовываться структура групп. Ещё не ясно, сколько локальных доменных групп нужно будет создать, поскольку это зависит от количества общих папок, принтеров, требований к разграничению доступа и т.п. Но количество глобальных групп примерно ясно. Учитывая, что их основным назначением является группировка пользователей с одинаковыми требованиями, можно предположить, что за основу будет взята схема, где каждому подразделению соответствует своя глобальная группа:

- Дирекция.
- Торговый отдел.
- Маркетинг.
- Склад.
- IT.
- Контрактники.

Несмотря на то, что в компании в каждый момент времени работает не более одного контрактника, в соответствии с выбранной стратегией мы создадим для него отдельную группу. Положение, при котором контрактник всегда будет один, может измениться в любой момент, а мы к этому уже будем готовы.

11.3.1. Рекомендации по именованию групп

Имена групп в домене Active Directory должны быть достаточно описательными, содержательными и простыми. Учитывая, что иногда все три

условия могут казаться невыполнимыми, можно составлять названия групп согласно следующим правилам:

- Используйте английский язык.
- **В качестве первой буквы названия используйте букву, указывающую на тип группы (G, D или U).** Тип группы можно увидеть в настройке Active Directory — пользователи и компьютеры, и всё-таки лучше будет обозначить его ещё и в имени группы.
- **В названии глобальной группы приведите название подразделения, для которого вы эту группу создаёте.** Например, `Shop`, `Marketing`, `Store`, `Managers` и т.д..
- **В названии локальной доменной группы приведите назначение группы, по возможности — разрешения на доступ.** Поскольку локальные доменные группы используются для настройки прав доступа к различным ресурсам, следует отразить это в названии группы.

В качестве примера названия локальной доменной группы, которая будет давать доступ к печати на принтере, можно привести название D Printers. Примером названия глобальной группы для контрактников будет G Temporary, а локальной доменной группы, дающей группе администраторов полный доступ к какой-либо папке, — D Admins Full Control.

11.3.2. Управление членством в группах

Новая учётная запись пользователя автоматически помещается в группу Domain Users. Это группа по умолчанию, и в сетях, где не используется других операционных систем, кроме Windows, менять ее не нужно. При использовании других операционных систем руководствуйтесь рекомендациями производителей этих операционных систем. Мы же считаем, что у нас однородная сетевая среда, включающая только компьютеры с Windows. Из группы по умолчанию пользователя удалить нельзя.

Примечание.

Новая учётная запись компьютера автоматически помещается в группу Domain Computers.

Учётная запись как пользователя, так и компьютера, может быть членом любой группы, поскольку группы не подразделяются в зависимости от типа содержащихся в них записей (см., например, системные группы Everyone и Authenticated Users).

По умолчанию членство в доменных группах имеет право изменять только член группы администраторов домена. Это привилегированная группа с наибольшими полномочиями в своем домене. Если доменное простран-

ство растёт и достигает нескольких сотен пользователей, скорее всего, к тому моменту администраторы сети уже будут иметь достаточно опыта и управление принадлежностью к группе будут рассматривать как обычное дело, которое мог бы выполнить и кто-нибудь менее опытный.

Домен Active Directory даёт возможность свалить эту работу на кого-нибудь другого. Имеет смысл заранее спланировать управление группами и уже при создании домена распределить обязанности по управлению членством между пользователями.

Чтобы передать полномочия по управлению членством в группе одному из состоящих в ней пользователей, выполните следующие действия:

1. Зарегистрируйтесь на SRVR001 как администратор и запустите консоль **Active Directory — пользователи и компьютеры**. Вызовите окно свойств любой доменной группы и перейдите на вкладку **Управляется**.
   Нажав на кнопку **Изменить**, вы можете ввести или выбрать имя пользователя (но не группы), который будет отвечать за эту группу. После этого в свойствах группы появится указание на того, кто является ее администратором, но у этого пользователя всё ещё нет необходимых полномочий.
2. Для того чтобы дать пользователю эти полномочия, установите флажок **Менеджер может изменять членство в группе**.
3. Нажав на кнопку **OK**, закройте окно свойств группы.

11.3.3. Влияние изменения членства в группе на работу пользователя. Использование «пропуска»

Пользователь может получать разрешение на доступ к ресурсам или прямо (через учётную запись), или через членство в группе. Первый способ не является универсальным решением, и администраторам рекомендуется применять его только в исключительных случаях. Наделение полномочиями групп ведёт к облегчению всего процесса управления и к упрощению системы сети.

Пусть у нас имеется глобальная группа для торгового отдела с именем G Shop, а в сети сейчас работает пользователь `Shop1` — член этой группы. Пока он работает, мы создаем для торгового отдела новую папку и предоставляем к ней доступ на чтение и запись группе G Shop.

Примечание.

Речь идёт о неоптимальной стратегии A → G ← P, которую мы используем только в целях иллюстрации принципа.

Создав общую папку, мы объявляем торговому отделу о том, что доступ к ней открыт. Пользователь `Shop1` немедленно пытается открыть эту папку и терпит неудачу.

Что произошло, ведь `Shop1` входит в группу, имеющую нужное разрешение? Для ответа на этот вопрос рассмотрим подробнее, как именно происходит проверка полномочий пользователя при попытке доступа к ресурсу.

Создание и использование пропуска

При регистрации пользователя в домене для него на основании данных из учетной записи создастся «пропуск» (security access token). Это внутренняя структура операционной системы, которая формируется в следующем порядке:

1. Контроллер домена, который проводит регистрацию, записывает первую часть пропуска: регистрационное имя пользователя и его идентификационный код (SID).
2. Потом в пропуск записывается список групп, членом которых является данный пользователь. Список глобальных и локальных групп, членом которых является данный пользователь, добавляет контроллер домена, список универсальных групп добавляет сервер глобального каталога.
3. Третью часть пропуска составляет список разрешений данной учётной записи в домене (примером такого разрешения является право изменить системное время). Этот список предоставляет контроллер домена.

Примечание.

Если домен Active Directory под управлением Windows 2000 работает в основном (native) режиме, то для создания пропуска необходим сервер глобального каталога. Если этого сервера нет, то пропуск не будет создан и пользователь не сможет зарегистрироваться. Исключением является случай, когда пользователь ранее работал на этом же компьютере: тогда информация для пропуска будет взята из кэша (если регистрация в домене через кэш не запрещена).

Каждый ресурс в системе имеет свой дескриптор безопасности — «турникет», которому пользователь должен предъявить свой пропуск при каждой попытке доступа к ресурсу. Если пропуск соответствует, то доступ будет разрешен.

Теперь вернемся к пользователю `Shop1`. Пытаясь открыть вновь созданную папку, он предъявил свой пропуск. Этот пропуск был сформирован,

когда он зарегистрировался в сети, то есть до того, как мы дали его группе разрешение на доступ к папке. Поэтому ему и отказано в доступе.

Теперь, чтобы получить свой законный доступ, пользователь должен завершить сеанс работы и зарегистрироваться заново. Перезагружать компьютер при этом не нужно.

Если бы вы предоставили доступ к новой папке не группе, а непосредственно пользователю (по учетной записи), то он получил бы доступ сразу же, без перерегистрации, поскольку учетная запись присутствует в пропуске всегда. В другую сторону это тоже работает: если вы лишаете доступа к ресурсу конкретного пользователя, то он лишается его сразу. Кстати, это практически единственный случай, когда управлять разрешениями уместно именно через учетную запись, а не через членство в группе.

Если вы хотите закрыть доступ пользователю, являющемуся членом группы, которой дано разрешение на доступ к какой-либо общей папке, у вас есть два пути:

- Закрытие доступа.
- Удаление пользователя из группы.

Обе возможности имеют свои плюсы и минусы, которые мы сейчас рассмотрим.

Закрытие доступа

Запрет некоторой возможности доступа (например, записи) не эквивалентен отсутствию соответствующего разрешения. Если разрешение этой возможности отсутствует (не указано явно), то его значение наследуется от родительской папки. А при явно указанном запрете разрешения родительской папки не играют роли. Таким образом, пользователь имеет разрешение на доступ к ресурсу только в том случае, если доступ ему разрешён и при этом не запрещён.

На вкладке **Безопасность** в окне свойств папки или файла в поле **Разрешения** есть столбец **Запретить**. Чтобы запретить доступ пользователю `Shop1`, не меняя прав его группы, добавьте этого пользователя в список управления доступом и поставьте флажок в клетке **Полный доступ/Запретить**. Все разновидности доступа к ресурсу будут для него мгновенно закрыты.

Преимуществом этого способа является его мгновенное действие, причем без всякой помощи со стороны пользователя, а недостатком — некоторое усложнение схемы разрешений в системе.

Удаление пользователя из группы

Этот способ вы можете применять в том случае, если нужно закрыть пользователю доступ ко всем ресурсам, на которые он имеет право как член группы. Если некоторые ресурсы ему еще нужны, создайте группу, дающую доступ только к ним, и переместите пользователя в нее.

Пусть, например, группа сотрудников торгового отдела (`G Shop`) через членство в локальной доменной группе XXX получает доступ к папке с договорами, а через членство в локальной доменной группе УУУ — к печати на принтере, и пусть некоего сотрудника уволили. Необходимо немедленно закрыть ему доступ к договорам, но оставить доступ к принтеру, чтобы он смог распечатать результаты своей работы. Если вы удалите его из группы `G Shop`, то после перерегистрации он потеряет доступ и к папке с договорами, и к сетевому принтеру.

11.4. Итоги

Права доступа к ресурсам следует настраивать не для отдельных пользователей, а для целых групп, иначе сетевая среда постепенно окажется безнадежно запутанной.

В домене существует две разновидности групп: группы безопасности и группы распространения. Для групп безопасности можно настраивать права доступа, а группы распространения предназначены только для рассылки сообщений электронной почты.

Группы безопасности подразделяются в соответствии с областью их видимости. Назначением глобальных групп является группировка пользователей со сходными требованиями к ресурсам. Локальные доменные группы предназначены для настройки прав доступа к сетевым ресурсам. Универсальные группы применяются в крупных сетях с целью облегчения управления доступом.

Список членов глобальных и локальных доменных групп хранится на контроллерах домена, в котором созданы эти группы, а членство в универсальных группах хранится на всех серверах глобального каталога леса Active Directory. Группы могут входить в группы такого же или другого типа, эта возможность зависит от режима работы домена.

При разрешении доступа следует придерживаться рекомендованных стратегий, поскольку только так можно сохранить ясность в сети независимо от её величины. Наиболее часто применяется стратегия

$$A \rightarrow G \rightarrow DL \leftarrow P$$

По умолчанию управлять членством в группах имеют право администраторы домена и члены группы Account Operators. Однако можно создать Администратора группы, который будет отвечать за её деятельность и производить изменения по мере необходимости.

При попытке доступа к некоторому ресурсу операционная система проверяет «пропуск» пользователя, формируемый в ходе регистрации его в домене на основе учетной записи, списка групп, членом которых является эта учетная запись, и доменных разрешений. Если пользователь входит в несколько десятков групп, может случиться, что процесс регистрации несколько затормозится. Поэтому следует тщательно планировать членство в группах и использовать тот факт, что группы могут быть членами других групп.

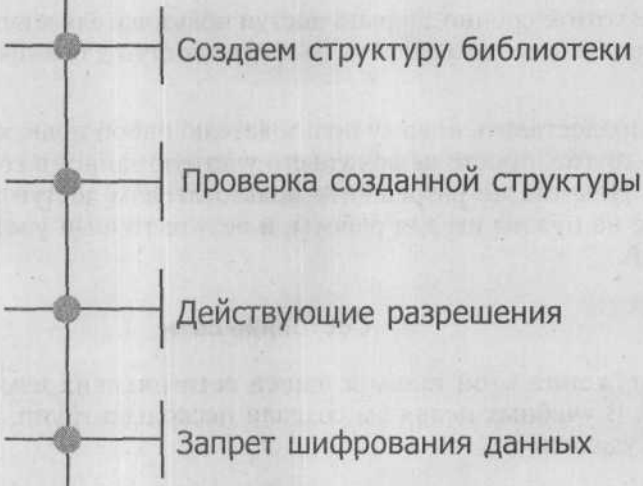
Если вы хотите срочно закрыть доступ пользователя к некоторому ресурсу, то проще всего это сделать, запретив доступ для конкретной учетной записи.

Чтобы предоставить новому пользователю набор прав, которым уже обладают другие, просто включите его учетную запись в соответствующую группу. Никогда не разрешайте пользователям доступ к тем ресурсам, которые не нужны им для работы, и ведите точный учет выданных разрешений.

Состояние сети

На протяжении этой главы в нашей сети никаких изменений не произошло. В учебных целях вы создали несколько групп, которые теперь можете удалить.

Глава 12 Создаем хранилище документов предприятия



Каждая организация развивается, и одним из аспектов развития является накопление документов. Встает вопрос об их централизованном хранении. Разумеется, было бы удобно хранить все важные документы в электронном виде. Место, где мы будем хранить документы в электронном виде, назовем хранилищем данных.

Способы хранения документов могут быть разнообразными, и это касается не только места их хранения, но и формата данных и инструментов поиска и просмотра документов. Часто документы хранятся в обычной базе данных. Другие распространенные способы хранения — общедоступные папки системы Microsoft Exchange Server или применение технологии Microsoft SharePoint Portal Server

Хранилище документов, подобно самому предприятию, будет развиваться. В начале своей деятельности далеко не каждая организация может позволить себе вкладывать деньги в новейшие технологии обработки документов, поэтому малые фирмы обычно начинают с обыкновенных разделяемых папок на сервере. В этой главе мы рассмотрим оптимальную реализацию этого простейшего способа хранения документов.

При работе с документами всегда важно помнить о том, что ценность содержащейся в них информации может быть очень высока. Поэтому документы нужно хорошо «спрятать», обеспечив доступ к ним только тем сотрудникам, которым это необходимо, а также защитить информацию от хищения и потери при сбоях программного и аппаратного обеспечения.

12.1. Создаем структуру библиотеки

Очень важно заранее продумать структуру хранилища данных. Она должна удовлетворять следующим требованиям:

- **Простота.** Хранилище данных должно быть простым в использовании и легко поддаваться администрированию.

- **Прозрачность.** Принцип систематизации данных должен быть понятен как администратору, так и пользователю. Важно, чтобы пользователь мог с первого взгляда определить, где и в какой части хранилища находится информация того или иного типа.
- **Безопасность.** В любой момент может возникнуть необходимость защитить некоторую часть хранилища дополнительными мерами безопасности.
- **Иерархическая структура.** Чтобы обеспечить возможность дальнейшего расширения с сохранением наглядности, данные должны быть организованы иерархически.
- **Масштабируемость.** Хранилище должно легко поддаваться увеличению в связи с ростом объема хранящихся документов, географическим расширением предприятия или увеличением разнообразия видов его деятельности.
- **Удобство резервного копирования.** Хотя архивирование входит в понятие безопасности, всё же следует вынести его отдельным пунктом. При планировании хранилища необходимо оценить, насколько просто будет архивировать и восстанавливать как хранилище целиком, так и отдельные его части.

Помните, что хранилище документов предназначено для того, чтобы облегчить работу пользователей, а не затруднить ее, поэтому планируйте структуру данных, исходя из их производственных потребностей.

Вспомним организационную структуру нашего учебного предприятия Study. В нем работают три руководителя, пять сотрудников в торговом отделе, три сотрудника в отделе маркетинга, трое на складе и один администратор сети. Иногда к этим работникам добавляется один временный.

Часы работы предприятия с понедельника по пятницу с 8.00 до 16.00, а склад открыт круглосуточно.

12.1.1. Технологическое решение

Поскольку наше предприятие пока не может купить современное программное обеспечение для обработки документов, выберем простейшее решение — хранение файлов в разделяемых папках — и посмотрим, удовлетворяет ли оно вышеприведенным требованиям.

- **Простота.** Для администратора нет ничего проще создания папки, а пользователи могут обращаться к этим папкам по сети, указывая UNC-путь `\\server\folder\subfolder`.
- **Прозрачность.** Названия папок отражают их принадлежность к отделу и тип хранимых документов.
- **Безопасность.** Разместив папки на файловой системе NTFS, мы можем ограничить доступ к ним средствами разрешений NTFS.

- **Иерархическая структура.** В папке, например, торгового отдела создадим подпапки «Шаблоны документов», «Договоры», «Счета» и т.п. Можно так настроить разрешения, чтобы новые уровни иерархии могли создавать сами пользователи из данного отдела.
- **Масштабируемость.** Количество папок в разделе, отформатированном файловой системой NTFS, ограничено, но настолько большим числом, что для нашего предприятия это ограничение несущественно.
- **Удобство резервного копирования.** Резервное копирование файловой системы — стандартная задача, решаемая стандартными системными средствами. Архивирование как всей файловой системы, так и отдельных ее частей можно выполнять автоматически.

Оказывается, даже простейшее решение удовлетворяет всем нашим требованиям. Следующим важным шагом будет создание масштабируемой структуры.

12.1.2. Структура хранилища данных

При планировании иерархической структуры очень важно решить, по какому принципу подразделять данные на верхнем уровне иерархии. Возможны следующие варианты:

- **По назначению документов.** При этом папки верхнего уровня назывались бы «Договоры», «Счета-фактуры», «Накладные», «Протоколы правления» и т.п., а подпапки каждой из этих папок назывались бы по именам отделов. Преимуществом такого решения является очевидность разделения документов на категории, а серьезным недостатком — трудность разграничения доступа.
- **По географическому расположению.** В предприятии с несколькими филиалами папки верхнего уровня могли бы называться «Санкт-Петербург», «Выборг», «Москва». Преимущество — простота ориентирования сотрудников в структуре предприятия, а недостаток — сложность управления хранилищем. Кроме того, если сеть правильно выстроена, пользователи не смогут сразу распознать, в каком из отделов они сейчас работают. Всё выглядело бы одинаково с любого места.
- **По организационной структуре.** При этом папки верхнего уровня именовались бы по названиям подразделений. Преимущество — неограниченная масштабируемость, удобство для пользователей и возможность разграничить доступ стандартными средствами операционной системы, а недостаток — сложность реструктуризации при изменении структуры предприятия.

Рекомендуется привлечь к разработке будущей структуры хранилища руководителей подразделений, но последнее слово должно остаться за

администратором сети, потому что именно ему придется эту структуру строить, поддерживать и расширять.

Решение для нашей сети

Для учебного предприятия Study выберем структуру данных, копирующую структуру организационную. Таким образом, на верхнем уровне будет шесть папок:

- «Дирекция».
- «Продажи».
- «Маркетинг».
- «Склад».
- «IT».
- «Прочие».

Администратору придется шесть раз выполнить действия по открытию сетевого доступа к папке и шесть раз настроить разрешения, а пользователи, введя в окне **Пуск → Выполнить** путь `\\SRVR001`, увидят шесть общих папок.

Более экономным решением было бы разместить эти шесть папок не на первом уровне иерархии, а на втором, создав их как подпапки, например, папки «Library». Имя этой объемлющей папки должно иметь смысл для администратора, а пользователи будут знать ее только под сетевым именем («Библиотека»), которое может отличаться от локального. Теперь, введя путь `\\SRVR001`, пользователь увидит одну общую папку, а не шесть.

Скрытые общие папки

Когда пользователь вводит путь `\\SRVR001`, он видит все общие папки, расположенные на сервере. Может случиться так, что некоторые из них вы завели для обмена данными с коллегами-администраторами, а рядовым пользователям знать о них не следует. Например, это папка с музыкой или фильмами. Вы, конечно, можете спрятать ее под именем `AdminTools` и настроить разрешения так, чтобы открыть ее было невозможно, но рано или поздно аудитор предприятия попросит вас предъявить ее содержимое.

Чтобы надежно спрятать такую сетевую папку, нужно сделать ее скрытой. Скрытые папки отличаются от обычных разделяемых папок тем, что увидеть их можно, только зная точное сетевое имя. По команде **Пуск → Выполнить** `\\server` эти папки не отображаются.

Сетевое имя скрытой папки должно заканчиваться знаком $. То есть коллега-администратор, введя полный путь `\\SRVR001\Music$` (без различия заглавных и строчных букв), увидит вашу папку, а аудитор не узнает о ее существовании.

12.1.3. Создание структуры хранилища

Создание и конфигурирование общих папок

Выполните следующую последовательность действий:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Запустите консоль **Пуск → Администрирование → Управление компьютером**. Разверните ветвь **Служебные программы → Общие ресурсы** (рис. 12.1). В правой части окна консоли вы увидите имеющиеся общие папки.
3. Правой кнопкой мыши щелкните по папке **Общие ресурсы** и из контекстного меню выберите команду **Новый общий ресурс**. Запустится Мастер создания общих ресурсов.
4. Нажмите на кнопку **Далее** и в поле **Путь к папке** задайте путь `C:\Library`. После нажатия на кнопку **Далее** появится сообщение об отсутствии заданной папки с запросом на ее создание. Нажатием на кнопку **Да** подтвердите ее создание.
5. В окне **Имя, описание и параметры** оставьте значения по умолчанию (рис. 12.2) и нажмите **Далее**.
6. В окне **Разрешения** установите значение **У всех пользователей доступ только для чтения** и нажмите на кнопку **Готово**. В ОС Windows Server 2003 это значение установлено по умолчанию, а в Windows 2000/XP по умолчанию всем предоставляется полный доступ к новой общей папке.

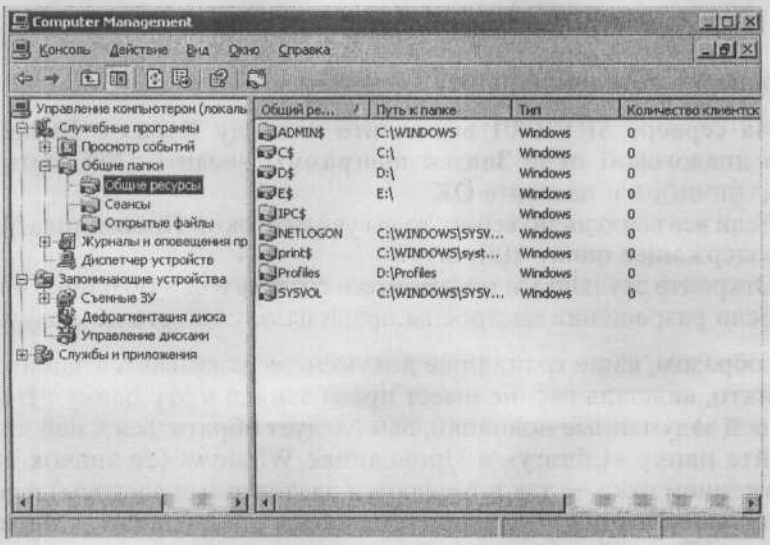


Рис. 12.1. *Общие папки в окне консоли* ***Управление компьютером***

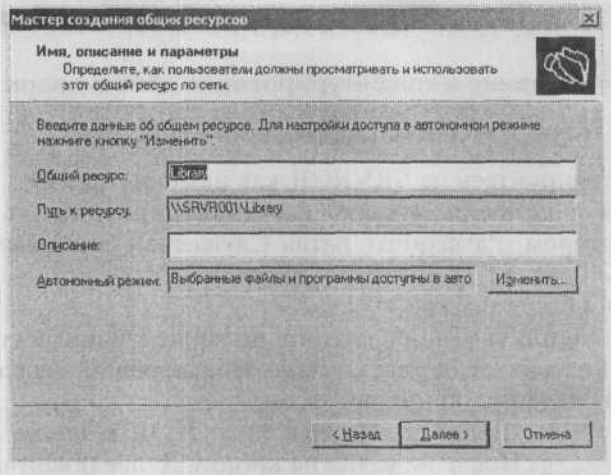


Рис. 12.2. *Мастер общих ресурсов.*

7. В итоговом окне вы увидите всю конфигурацию общей папки. Нажмите **Готово.**

Общую папку можно было создавать и из Проводника Windows. Хотя процесс с использованием консоли **Управление компьютером** может показаться несколько длительным, рекомендуем применять именно этот способ, потому что для создания общей папки на удаленном компьютере (не том, за которым вы работаете) пригоден только он.

Проверка созданной папки

Для проверки созданной папки:

1. На сервере SRVR001 выполните команду **Пуск → Выполнить** и в диалоговом окне **Запуск программы** введите UNC-путь в виде `\\SRVR001` и нажмите **OK**.
2. Если все выполнено верно, то вы увидите окно Проводника Windows, содержащее папку «Library».
3. Откройте эту папку и попытайтесь создать в ней подпапку или файл. Если разрешения настроены правильно, у вас это не получится.

Таким образом, ваше хранилище документов оказывается защищено: по сети никто, включая вас, не имеет права записи в эту папку. Чтобы создать в ней задуманные подпапки, вам следует обратиться к ней локально. Откройте папку «Library» в Проводнике Windows (ее значок снабжен изображением руки — так помечаются разделенные ресурсы) и создайте в ней запланированные подпапки «Дирекция», «Продажи», «Маркетинг», «Склад», «IT» и «Прочие».

12.1.4. Настройка разрешений NTFS

Обдумывая схему разграничения доступа пользователей к документам, обратите внимание на следующие моменты:

- **Кто будет управлять хранилищем.** Следует позаботиться о том, чтобы группе пользователей, отвечающих за управление структурой библиотеки документов, было предоставлено разрешение «Полный доступ». Такие же полномочия должны быть предоставлены администраторам.
- **Какой уровень доступа к документам нужен пользователям.** Обычно для каждой папки настраивают два уровня доступа: для чтения и для редактирования содержимого.
- **Проверка разрешений.** Сразу же после установки или смены разрешений необходимо проверить, правильно ли они настроены (не забыли ли вы чего-то, нет ли нежелательных эффектов, порожденных наследованием или отменой наследования).
- **Как предоставлять доступ отдельным пользователям.** Как показано в главе 11, разрешения необходимо предоставлять не отдельным пользователям, а группам. С ростом сети вы сами убедитесь в обоснованности этого правила.

Обычно в небольших компаниях хранилищем документов управляют члены группы администраторов домена, но мы, чтобы все было по правилам, создадим для этой цели отдельную группу, в которую впоследствии можно будет включить кого-нибудь из опытных пользователей, свалив на него одну из администраторских обязанностей.

Учитывая независимость подразделений и необходимость двух уровней доступа, для каждой подпапки папки «Library» создадим две локальных доменных группы.

Далее предположим, что руководству предприятия нужен не только полный доступ к собственным документам, но и право чтения документов остальных подразделений.

Ограничивать доступ к подпапкам мы будем на уровне разрешений NTFS, а в качестве сетевого разрешения предоставим всем «Полный доступ». Для большей безопасности это право нужно дать не группе «Все» («Everyone»), а группе «Domain Users» — встроенной группе, в которой состоят все пользовательские учетные записи. Группу «Все» нужно удалить из списка пользователей и групп, для которых настроены сетевые разрешения на папку «Library».

Какие понадобятся группы

Мы договорились применить стратегию **A → G → DL ← P**, и теперь нужно создать локальные доменные группы, для которых будут настроены раз-

решения, и глобальные группы, через которые пользователи получат эти разрешения. В соответствии с требованием двух уровней доступа к папке каждого подразделения, для каждой из них создадим по две локальных доменных группы.

1. Запустите консоль **Active Directory — пользователи и компьютеры.**
2. В контейнере **Пользователи** создайте локальные доменные группы со следующими именами:

   D Library Admin
   D Library IT Read
   D Library IT Write
   D Library Marketing Read
   D Library Marketing Write
   D Library Shop Read
   D Library Shop Write
   D Library Other Read
   D Library Other Write
   D Library Store Read
   D Library Store Write
   D Library Managers Read
   D Library Managers Write

Совет.

Если у вас не шесть подразделений, а полсотни, то создание групп с похожими именами через графический интерфейс может оказаться несколько утомительным. Напоминаю, что в ОС Windows Server 2003 в отличие от Windows 2000/XP включена утилита командной строки DSADD, предназначенная для создания в активном каталоге объектов разного типа. Для создания группы (например, D Library IT Read) ее нужно запускать со следующими аргументами:

```
dsadd group CN="D Library IT Read", CN=Users, DC=study,
DC=local -scope l
```

Справку об утилите DSADD можно получить, введя команду **dsadd /?.**

3. Пользователей будем группировать по подразделениям и по степени «продвинутости», а кроме того, создадим группу администраторов хранилища. В контейнере **Пользователи** создайте глобальные группы со следующими именами:

   G Library Admin
   G IT regular
   G IT power
   G Marketing regular
   G Marketing power
   G Shop regular
   G Shop power

G Other regular
G Other power
G Store regular
G Store power
G Managers regular
G Managers power

Совет.

Чтобы создать эти группы из командной строки, воспользуйтесь утилитой DSADD. Запускать ее нужно со следующими аргументами:

```
dsadd group CN="G IT power", CN=Users, DC=study, DC=local -scope g
```

Теперь распределим учетные записи пользователей по этим глобальным группам. Условно считаем, что в каждом подразделении пользователь с наибольшим номером в регистрационном имени является опытным, и включаем таких пользователей в соответствующую группу `G...power`, а всех остальных пользователей — в группы `G...regular`. Некоторые группы при этом останутся пустыми. В группу `G Library Admin` включите пользователя `Marketing3`.

Разрешения для корневой папки

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Откройте вкладку **Безопасность** в окне свойств папки «Library». Нажмите кнопку **Дополнительно** и снимите флажок **Наследовать от родительского объекта.**
3. Из списка субъектов доступа удалите всех имеющихся там пользователей и группы последовательным нажатием кнопки **Удалить.**
4. Вместо них добавьте в список следующие группы со следующими правами:
   - `Администраторы`: полный доступ.
   - `D Library Admin`: полный доступ.
   - `Domain Users`: чтение, чтение и выполнение, просмотр содержимого папки.

Разрешения для папок подразделений

Напоминаю, что мы спланировали следующий порядок доступа: сотрудники каждого подразделения должны иметь доступ к папке своего отдела (одни только на чтение, другие на запись), руководство кроме этого должно иметь возможность читать любую папку, а администраторам домена и администраторам хранилища следует предоставить полный доступ. Разрешения будем настраивать для локальных доменных групп.

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Откройте вкладку **Безопасность** в окне свойств папки «Library\IT». Нажмите кнопку **Дополнительно** и снимите флажок **Наследовать от родительского объекта.**
3. На вкладке **Безопасность** в списке субъектов доступа выделите группу Domain Users и нажмите кнопку **Удалить.**
4. Вместо нее добавьте в список следующие группы со следующими правами:
   - `Администраторы`: полный доступ.
   - `D Library Admin`: полный доступ.
   - `D Library IT Read`: чтение, чтение и выполнение, просмотр содержимого папки.
   - `D Library IT Write`: «Изменить».
5. Нажатием на кнопку **ОК** закройте диалоговое окно свойств папки «Library\IT».

Проделайте то же самое с папками «Дирекция», «Продажи», «Маркетинг», «Склад» и «Прочие», настраивая разрешения для соответствующих локальных групп «...Read» и «...Write». Разрешение руководству на чтение всех папок настроим на следующем шаге.

Применение стратегии A → G → DL ← P

Последним шагом настройки разрешений является включение глобальных групп в нужные локальные доменные группы. Для спланированной нами схемы доступа членство в группах должно быть настроено так, как показано в табл.12.1. Инструментом для изменения членства групп служит консоль **Active Directory — пользователи и компьютеры.**

Членство глобальных групп в локальных доменных группах *Таблица 12.1*

Локальная доменная группа	Входят
D Library Admin	G Library Admin
D Library IT Read	G IT regular, G Managers regular, G Managers power
D Library IT Write	G IT power
D Library Marketing Read	G Marketing regular, G Managers regular, G Managers power
D Library Marketing Write	G Marketing power
D Library Shop Read	G Shop regular, G Managers regular, G Managers power
D Library Shop Write	G Shop power
D Library Other Read	G Other regular, G Managers regular, G Managers power
D Library Other Write	G Other power
D Library Store Read	G Store regular, G Managers regular, G Managers power
D Library Store Write	G Store power
D Library Managers Read	G Managers regular
D Library Managers Write	G Managers power

Можно ли было построить группы проще, включив, например, глобальные группы опытных пользователей в соответствующие глобальные группы рядовых? В домене с режимом Windows 2000 native или Windows Server 2003 — можно, но наш домен пока работает в смешанном режиме, в котором не допускается членства глобальных групп в других глобальных группах.

12.1.5. Настройка сетевых разрешений

Открывая общий доступ к папке «Library» под сетевым именем «Библиотека», мы дали группе «Все» только разрешение на чтение. Это значит, ни один пользователь, подключающийся к данной папке по сети, не получит больше прав, как бы ни были настроены для него разрешения NTFS. Чтобы работали именно эти разрешения, доступ по сети следует открыть как полный. Для какой группы? Возможны варианты:

- **Встроенная группа «Все» («Everyone»).** В эту группу входят все учетные записи пользователей, включая гостевую. Поскольку мы отключили встроенную учетную запись «Гость», предоставление полного доступа этой группе довольно безопасно.
- **Встроенная группа «Зарегистрированные пользователи» («Authenticated Users»).** В эту группу гостевая учетная запись не входит, поэтому с точки зрения безопасности правильнее открыть доступ именно этой группе. Вдруг вы впоследствии для какой-то особой цели временно включите гостевую учетную запись и забудете ее отключить?

Откройте вкладку **Доступ** в диалоговом окне свойств папки «Library» и нажмите кнопку **Разрешения**. Из списка субъектов доступа удалите группу «Все» и добавьте группу «Зарегистрированные пользователи», которой предоставьте разрешение «Полный доступ».

12.2. Проверка созданной структуры

Так как создаваемая нами библиотека предназначена для организации доступа к документам по сети, то проверять ее функционирование и правильную настройку разрешений следует с клиентского компьютера.

Убедимся, что пользователь `Store3` имеет возможность создавать документы в папке «Склад», но не в других папках; пользователь `Manager1` может читать документы в любой папке, но не имеет права на создание и удаление файлов даже в собственной папке; пользователь `Marketing3` как администратор библиотеки имеет право создавать и удалять файлы из всех папок.

Для проверки зарегистрируйтесь на PC001 под именем рядового пользователя, выполните команду **Пуск → Выполнить** и в поле **Открыть** введите путь `\\SRVR001\Библиотека`.

12.3. Действующие разрешения

Как администратору файлового сервера вам рано или поздно придется выслушивать жалобы пользователей на неправильно, с их точки зрения, настроенные права доступа к данным (обычно жалуются на недостаток, а не на избыток прав). Вам придется проверять, соответствуют ли действующие (полученные в сумме, через членство в разнообразных группах) разрешения политике предприятия.

В ОС Windows версий более ранних, чем XP Professional, вам пришлось бы открыть вкладку **Безопасность** в окне свойств конкретного ресурса и выписать список групп — субъектов доступа — с их разрешениями; затем открыть консоль **Active Directory — пользователи и компьютеры** и проверить, в каких группах пользователь состоит непосредственно или через членство группы в группе; затем вычислить действующие разрешения для данного пользователя. Все окажется еще более трудоемко, если речь идет не о стандартных («Чтение», «Изменение» и т.п.), а об особых разрешениях NTFS.

В ОС Windows Server 2003 и Windows XP Professional существует возможность посмотреть на действующие разрешения конкретного пользователя непосредственно:

1. На вкладке **Безопасность** окна свойств нужного ресурса нажмите кнопку **Дополнительно**.
2. В окне **Дополнительные параметры безопасности** перейдите на вкладку **Действующие разрешения**.
3. Нажмите кнопку **Выбрать**, выберите нужного пользователя и просмотрите результат применения всех разрешений, полученных через его членство в группах.

Стоит напомнить, что действующие разрешения NTFS — это еще не окончательные права пользователя на доступ к данному ресурсу. Они взаимодействуют с правами доступа к разделяемому ресурсу по сети, которые вам следует проверить (при необходимости изменить) вручную.

12.4. Запрет шифрования данных

По умолчанию пользователи ОС Windows 2000 Professional и Windows XP Professional имеют право шифровать те файлы, к которым у них есть разрешение как минимум на запись. Зашифрованный файл доступен для прочтения только тому, кто его зашифровал. Ничего страшного, если пользователь шифрует личные документы в своей домашней папке, но если он проделает это с файлом в хранилище, к которому должны иметь доступ и другие пользователи, то это может нарушить нормальную работу предприятия.

Система Windows XP Professional предоставляет, правда, возможность указать, кто еще будет иметь доступ к зашифрованному файлу, но такое решение нельзя назвать системным, потому что администратор не способен в это вмешаться. Можно запретить шифрование вообще, но этот запрет будет распространяться и на личные документы пользователя, что не всегда уместно. Единственное системное решение — это запрет шифрования файлов в конкретной папке.

Способ, который мы используем в хранилище документов, известен начиная с ОС Windows 2000. Он состоит в помещении в папку, в которой мы хотим запретить шифрование, файла DESKTOP.INI следующего содержания:

```
[Encryption]
Disable=1
```

Скопируйте этот файл во все папки подразделений. Не лишним будет защитить его дополнительно:

- Придайте файлу DESKTOP.INI атрибут «Скрытый» (установите флажок **Скрытый** на вкладке **Общие** окна свойств). Пользователи, для которых отключено отображение скрытых файлов, его не увидят.
- Настройте разрешения NTFS для этого файла так, чтобы удалить его могли только администраторы домена и администраторы хранилища.

12.5. Итоги

Хранение документов небольшого предприятия можно организовать в общих папках, расположенных на сервере. Структуру хранилища нужно тщательно продумать. Рекомендуется открыть сетевой доступ к одной папке, а для документов отдельных подразделений отвести ее подпапки. Далее нужно ограничить доступ к папкам подразделений и назначить группу пользователей, которая в дальнейшем будет администрировать хранилище документов.

Большая часть главы была посвящена настройке разрешений NTFS и применению стратегии A → G → DL ← P. Эта базовая стратегия обеспечивает простое и наглядное управление правами доступа и хорошо приспособлена к дальнейшему расширению сети. После настройки разрешений для подпапок последним шагом в организации хранилища является открытие сетевого доступа к папке верхнего уровня и назначение зарегистрированным пользователям права на полный доступ к ней по сети.

Права, которые конкретный пользователь имеет на конкретный ресурс, получаются сложным взаимодействием разрешений, унаследованных этим ресурсом от родительского объекта, и разрешений, полученных пользователем благодаря членству в разных группах, в том числе вложенных одна в другую. Результат взаимодействия называется действующими разрешениями. В ОС Windows XP Professional и Windows Server 2003 действующие разрешения конкретного пользователя на конкретный ресурс можно посмотреть на вкладке **Действующие разрешения** окна **Дополнительные параметры безопасности**, в операционных системах предыдущих версий их нужно вычислять вручную.

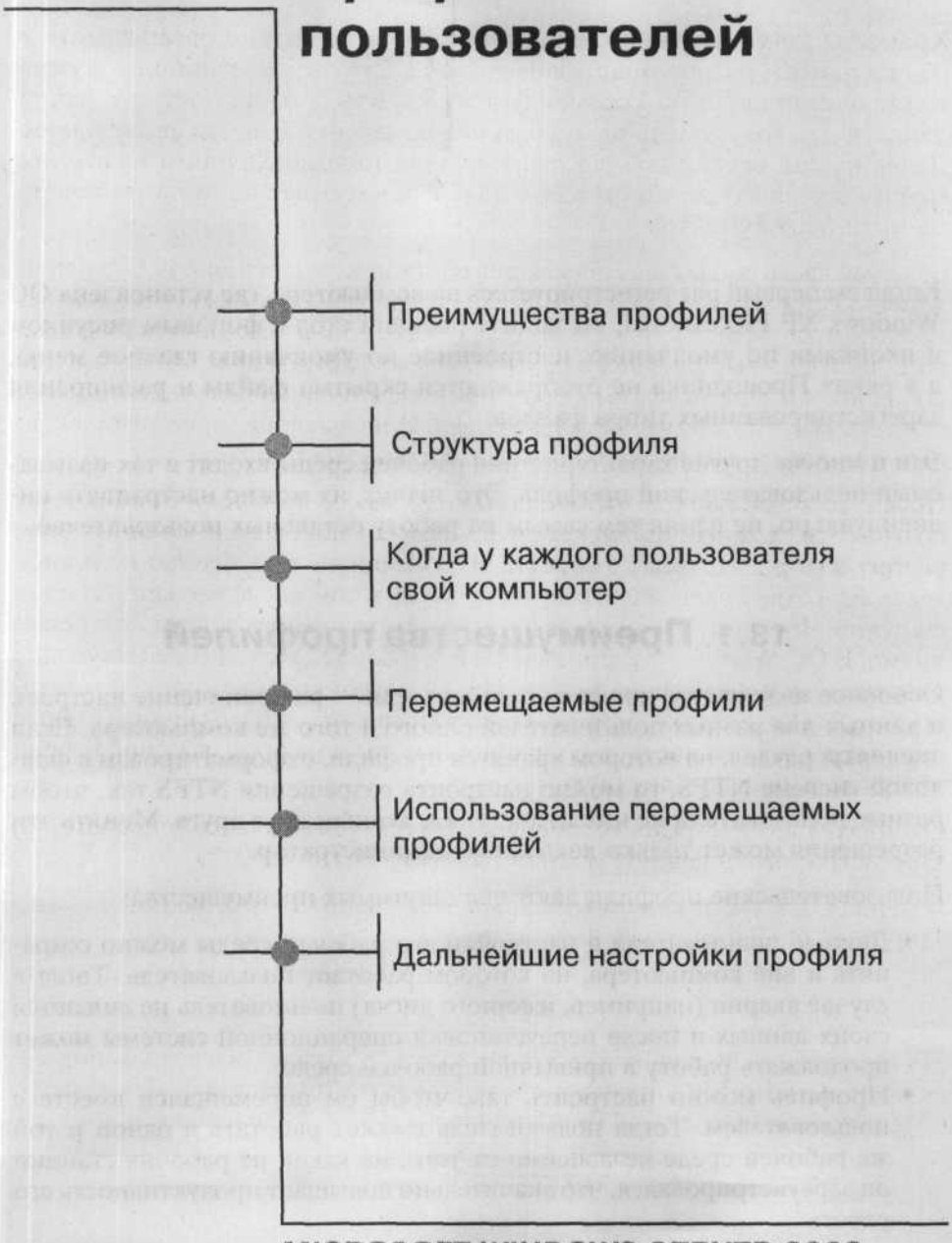
Окончательно настроив разрешения NTFS, обязательно проверьте их, зарегистрировавшись под именем рядового пользователя.

В папках, доступ к которым открыт нескольким сотрудникам, уместно запретить шифрование файлов.

Состояние сети

На сервере появилась разделяемая папка «Library», известная под сетевым именем «Библиотека», с подпапками «Дирекция», «Продажи», «Маркетинг», «Склад», «IT», «Прочие».

Глава 13 Профили пользователей



Когда вы первый раз регистрируетесь на компьютере, где установлена ОС Windows XP Professional, вы видите рабочий стол с фоновым рисунком и иконками по умолчанию, настроенное по умолчанию главное меню, а в окнах Проводника не отображаются скрытые файлы и расширения зарегистрированных типов файлов.

Эти и многие другие характеристики рабочей среды входят в так называемый пользовательский профиль. Это значит, их можно настраивать индивидуально, не влияя тем самым на работу остальных пользователей.

13.1. Преимущества профилей

Основное назначение профиля пользователя — разграничение настроек и данных для разных пользователей одного и того же компьютера. Если дисковый раздел, на котором хранятся профили, отформатирован в файловой системе NTFS, то можно настроить разрешения NTFS так, чтобы разные пользователи не имели доступа к данным друг друга. Менять эти разрешения может только локальный администратор.

Пользовательские профили дают два ощутимых преимущества:

- Данные пользователя и настройки его рабочей среды можно сохранять и вне компьютера, на котором работает пользователь. Тогда в случае аварии (например, жесткого диска) пользователь не лишается своих данных и после переустановки операционной системы может продолжать работу в привычной рабочей среде.
- Профиль можно настроить так, чтобы он перемещался вместе с пользователем. Тогда пользователь сможет работать в одной и той же рабочей среде независимо от того, на какой из рабочих станций он зарегистрировался, что значительно повышает продуктивность его работы.

Чтобы воспользоваться этими преимуществами, администратор должен произвести некоторые настройки, которым и посвящена эта глава.

13.2. Структура профиля

Пользовательский профиль содержит в себе огромное количество установок и данных пользователей. Знание о расположении его отдельных составляющих необходимо для любых манипуляций с профилем, устранения неполадок или настройки резервного копирования

Установки содержатся в двух местах: в системном реестре и в специальных папках файловой системы. Данные реестра в ОС Windows, начиная с версии NT, тоже можно экспортировать как обычный файл и импортировать обратно в реестр. Реестровая часть пользовательского профиля содержится в файле NTUSER.DAT, который при активации профиля (при регистрации пользователя) читается в реестр, точнее в его ветвь HKEY_CURRENT_USER.

Что хранится в реестре

Файл NTUSER.DAT содержит следующие настройки:

- **Настройки Проводника Windows** (например, сокрытие расширений зарегистрированных типов файлов или подключенные сетевые диски).
- **Параметры Панели задач** (например, присутствие панели быстрого запуска).
- **Установленные принтеры** (различные локальные и сетевые принтеры).
- **Настройки Панели управления.**
- **Рабочие панели** (их наличие и вид)
- **Стандартные программы** (наличие приложений и программ, содержащихся в группе **Стандартные** главного меню — например, калькулятора).
- **Настройки приложений** (некоторые приложения сохраняют свои настройки в ветви HKEY_CURRENT_USER — примером может служить главная панель приложений Microsoft Word 2000).

Что хранится в папках

Профиль каждого пользователя представляет собой иерархию папок, изображенную на рис. 13.1. В этих папках хранятся:

- **Application Data**: данные конкретных приложений, например, пользовательский словарь некоторой программы для обработки текста. Какие именно данные будут храниться здесь, решает производитель приложений.
- **Cookies**: Файлы Cookie штатного браузера Internet Explorer.

- **Local Settings**: настройки и данные приложений, которые не перемещаются вместе с профилем пользователя. Это могут быть либо данные, относящиеся только к конкретному компьютеру, либо данные большого объёма, перемещение которых по сети нецелесообразно.
  - Application Data: данные приложений, специфичные для данного компьютера.
  - History: история работы браузера Internet Explorer.
  - Temp: временные файлы.
  - Temporary Internet Files: автономный кэш Internet Explorer.
- **Документы:** папка по умолчанию для хранения личных документов пользователя.
  - Музыка: папка по умолчанию для хранения звуковых файлов.
  - Рисунки: папка по умолчанию для графических файлов.
- **Недавние документы**: ярлыки к файлам, открывавшимся последними.
- **Главное меню**: ярлыки приложений, которые можно запустить из меню «Пуск».
- **Избранное**: Интернет-ярлыки для быстрого открытия вебстраниц в браузере Internet Explorer.
- **Nethood**: ярлыки на объекты сетевого окружения.
- **Printhood**: ярлыки на принтеры.
- **SendTo**: ярлыки на места сохранения копий файлов.
- **Рабочий стол**: файлы и ярлыки, размещенные на рабочем столе.
- **Шаблоны**: ярлыки шаблонов.

Где находится профиль

В системах семейства Windows 2000/XP и Windows Server 2003 профиль пользователя по умолчанию располагается в папке `%SYSTEMDRIVE%\Documents and Settings\%username%`. В этой папке находятся файл NTUSER.DAT и иерархия папок, представленная на рис. 13.1.

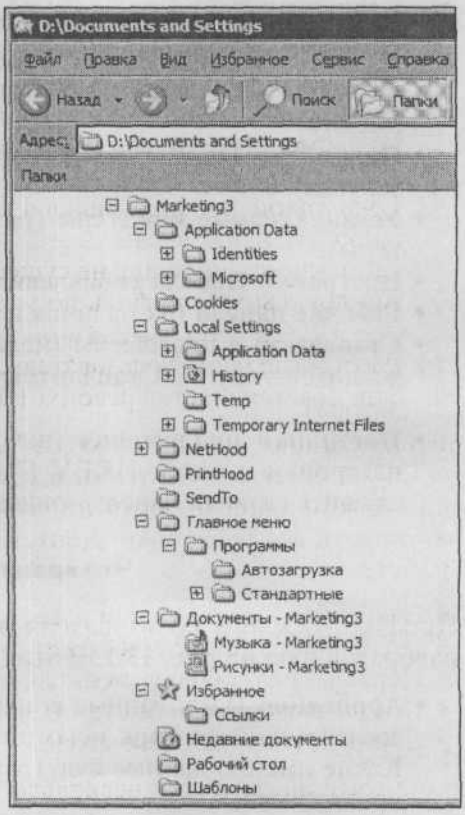


Рис. 13.1. *Папки профиля пользователя marketing3*

Исключение составляют компьютеры, на которых Windows XP Professional или Windows 2000 была установлена поверх Windows NT 4.0. После такого апгрейда профиль по умолчанию располагается в папке `%SYSTEMDRIVE%\WINNT\Profiles`.

13.3. Когда у каждого пользователя свой компьютер

После краткого, но от этого не менее важного вступления перейдём к практической части. Пусть пользователь `Shop1` впервые регистрируется на компьютере PC001. В этот момент компьютер выполняет следующие действия:

1. В ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList он попытается найти информацию о профиле пользователя `Shop1`. Поскольку пользователь `Shop1` на этом компьютере до сих пор не регистрировался, ссылки на профиль в реестре не существует, и компьютер продолжает поиск.
2. Если компьютер является членом домена, он проверит, существует ли «доменный» профиль в папке NETLOGON\Default User на контроллере домена.
3. Если такой профиль найден, он копируется во вновь созданную папку `%SYSTEMDRIVE%\Documents and Settings\Shop1`. Если же «доменного» профиля не существует, то в эту папку будет скопирован локальный профиль по умолчанию из папки `%SYSTEMDRIVE%\Documents and Settings\Default User`.
4. Реестровая часть пользовательского профиля (файл NTUSER.DAT) считывается в ветвь реестра HKEY_CURRENT_USER.

Теперь пользователь `Shop1` может настроить свою рабочую среду в соответствии со своими вкусами и служебными задачами. Поскольку никаких ограничений мы пока не вводили, пользователь может изменить практически все настройки. Допустим, он сконфигурировал следующие параметры:

- Отображать расширения известных типов файлов.
- Подключить сетевой диск Z:.
- Переключить главное меню на классический вид.
- Показывать панель быстрого запуска на панели задач.
- Сменить тему рабочего стола.

Кроме того, он поместил несколько файлов в папку «Мои документы».

После того, как пользователь `Shop1` завершит сеанс работы, эти настройки будут сохранены в его локальном профиле на жестком диске данного компьютера. При следующей регистрации этого пользователя на этом компьютере локальный профиль будет прочитан и настройки применены к новому сеансу, то есть пользователь сможет работать в той же самой рабочей среде.

Когда этот же пользователь впервые зарегистрируется на другом компьютере (PC002), все шаги по созданию локального профиля будут выполнены заново и в результате получится рабочая среда, не имеющая ничего общего со средой, настроенной на PC001. Пользователю придется вручную настраивать себе привычное окружение, поскольку не существует средств, которые могли бы обеспечить синхронизацию этих двух локальных профилей. Более того, ему понадобится синхронизировать содержание папки «Мои документы», что займет много времени.

Локальный администратор имеет возможность проверить все существующие локальные профили:

1. Зарегистрируйтесь на PC001 как администратор.
2. В главном меню щелкните правой кнопкой мыши по пункту **Мой компьютер** и из контекстного меню выберите команду **Свойства**.
3. Перейдите на вкладку **Дополнительно** и в части **Профили пользователей** нажмите кнопку **Параметры**. Откроется окно с профилями всех пользователей, которые зарегистрированы на этом компьютере.

Администратор может удалить из списка любой профиль, кроме своего собственного. Если вы не являетесь администратором, то в списке будет присутствовать только ваш профиль, который, понятно, тоже нельзя удалить. Таким образом, по наличию локального профиля можно судить о том, регистрировался ли на данном компьютере конкретный пользователь, а по дате последнего изменения узнать, когда именно: рядовой пользователь не имеет полномочий удалить эти сведения.

Локальные профили имеет смысл применять только тогда, когда каждый пользователь обеспечен отдельным компьютером, за которым большую часть времени и работает. При этом проблема одинаковой настройки рабочей среды на разных компьютерах просто не возникает.

Для нашего учебного предприятия такое решение не подходит. Сотрудникам отдела продаж приходится работать как в собственной комнате, так и за любым из компьютеров в торговом зале. Им нужна не только одинаковая рабочая среда на любом рабочем месте, но и доступ к одним и тем же документам через папку «Мои документы». Решением будет создание перемещаемых профилей.

13.4. Перемещаемые профили

Перемещаемым называется такой профиль, который «странствует» по узлам сети вместе с пользователем и вступает в силу на любом компьютере, на котором пользователь регистрируется. Перемещаемость профиля нужно указывать в свойствах доменной учетной записи. Для того, чтобы пользователь смог оценить преимущества перемещаемого профиля, должны быть выполнены следующие важные условия:

1. Перемещаемые профили должны храниться на компьютере, который постоянно доступен по сети (то есть включён и работает).
2. Этот компьютер с перемещаемыми профилями ни в коем случае не должен отвергать попытку подключения, то есть на нем должна быть установлена серверная операционная система с достаточным количеством лицензий на клиентский доступ.

В главе 4 мы создавали перемещаемый профиль в среде рабочей группы для локальной учетной записи. Сейчас наша сеть организована в домен, и порядок настройки перемещаемого профиля будет другим. Продемонстрируем его на примере пользователя `Shop2`.

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Создайте на диске C: папку «TravProfiles». Откройте сетевой доступ к этой папке и предоставьте группе «Зарегистрированные пользователи» («Authenticated Users») право полного доступа. Разрешения NTFS для этой папке и оставьте в исходном положении.
3. Запустите консоль **Active Directory — Пользователи и компьютеры** и отобразите свойства учетной записи `Shop2`.
4. Откройте вкладку **Профиль** и в поле **Путь к профилю** введите адрес `\\SRVR001\TravProfiles\Shop2`. Нажмите на кнопку **OK**.

Примечание.

Если вы настраиваете перемещаемый профиль не через графический интерфейс, а при помощи командного сценария ADSI (Active Directory Service Interfaces), то вместо регистрационного имени пользователя можете использовать переменную %username%.

13.4.1. Безопасность перемещаемых профилей

При первой регистрации пользователя `Shop2` в сети на сервере SRVR001 создаётся пустая папка профиля «Shop2». Она наполняется данными только по завершении сеанса работы пользователя. Разрешения NTFS для этой папки по умолчанию настроены так, чтобы доступ к ней имел

только соответствующий пользователь. Даже членам группы администраторов доступ запрещен.

В такой конфигурации администратор, желающий получить доступ к файлам профиля, должен стать владельцем этого профиля — папки и всей иерархии ее подпапок. Смена владельца может отрицательно повлиять на функционирование перемещаемых профилей. Это нежелательно, но в то же время доступ к профилям администратору нужен. Эта проблема решается при помощи групповой политики.

Чтобы при добавлении нового перемещаемого профиля администраторы автоматически получали полный доступ к нему, выполните следующие действия:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Запустите консоль **Active Directory — Пользователи и компьютеры**. Откройте окно свойств домена `study.local`.
3. Перейдите на вкладку **Групповая политика** и откройте объект **Default Domain Policy (Групповая политика по умолчанию)**.
4. Разверните ветвь **Конфигурация компьютера → Административные шаблоны → Система → Профили пользователей**. В правой части окна консоли выберите опцию **Добавить группу Administrators в перемещаемые профили пользователей (Add the Administrators security group to roaming user profiles)** и установите флажок **Включено**. Диалоговое окно закройте, нажав на кнопку **OK**.
5. Чтобы применить новую групповую политику, запустите утилиту командной строки GPUPDATE. После этого разрешения NTFS всех вновь создаваемых перемещаемых профилей будут включать полный доступ для членов группы администраторов.

13.4.2. Проверка созданного перемещаемого профиля

Проверка созданного нами перемещаемого профиля состоит из следующих этапов:

1. Зарегистрируйтесь на PC001 как пользователь `Shop2`.
2. Откройте окно свойств «Мой компьютер» и перейдите на вкладку **Дополнительно**. Нажмите кнопку **Параметры** в части **Профили пользователей** и убедитесь, что ваш профиль имеет **тип** «Перемещаемый».
3. Создайте на рабочем столе новый текстовый документ, а в папке «Мои документы» (меню **Пуск → Мои документы**) — новый файл типа «Звук Wav».

4. Завершите сеанс работы на PC001. В ходе завершения сеанса изменения в настройках профиля будут не только сохранены в локальном профиле пользователя `Shop2` на компьютере PC001, но и скопированы на сервер, в папку «TravProfiles».
5. Зарегистрируйтесь на SRVR001 как администратор. Откройте папку «TravProfiles\Shop2». Проверьте наличие текстового документа в подпапке «Рабочий стол» и звукового файла в подпапке «Документы».

13.4.3. Применение перемещаемого профиля

Возможно, вам приходила в голову идея, что если бы вы внутри профиля пользователя, размещенного на сервере, сохранили в папке «Рабочий стол» какой-нибудь новый документ, то пользователь увидел бы его сразу после начала работы. Что если использовать эту возможность для сообщения информации пользователям? Будет ли это работать? Давайте проверим.

1. Убедитесь, что пользователь `Shop2` не зарегистрирован ни на одном из компьютеров сети.
2. Как администратор, создайте в папке «`TravProfiles\Shop2\Рабочий стол`» на сервере новый документ MS Word.
3. Зарегистрируйтесь под именем `Shop2` на той рабочей станции, где вы в последний раз завершили сеанс как пользователь `Shop2`.

Если на этом компьютере установлена клиентская ОС Windows XP Professional, то вы увидите на рабочем столе новый документ. Но если на нем стоит Windows 2000, то новый документ отображен не будет. Это отличие объясняется порядком применения перемещаемых профилей в разных операционных системах.

Windows XP Professional

Если пользователь с перемещаемым профилем уже когда-либо регистрировался на данном компьютере, то при новой регистрации происходит следующее:

1. Операционная система находит в реестре информацию о том, что на данном компьютере уже сохранена локальная копия профиля.
2. Затем она считывает локальный файл NTUSER.DAT в ветвь реестра HKEY_CURRENT_USER.
3. Потом она сравнивает локальную копию профиля с версией на сервере и объединяет их. В результате отображается профиль в его истинном состоянии.

Windows 2000 Professional

Система Windows 2000 Professional в той же ситуации поступает иначе:

1. Операционная система находит в реестре информацию о том, что на данном компьютере уже сохранена локальная копия профиля.
2. Затем она сравнивает дату последнего изменения файлов NTUSER.DAT в локальном профиле и в папке перемещаемого профиля на сервере.
3. Перемещаемый профиль с сервера применяется локально только в том случае, когда файл на сервере более свежий. В противном случае применяется локальный профиль.

Вот и ответ на вопрос, почему созданный администратором в папке профиля документ не отобразился на рабочем столе. Чтобы принудительно ввести в силу изменения в перемещаемом профиле, вам нужно было бы обновить еще и файл NTUSER.DAT.

13.5. Использование перемещаемых профилей

Следует принять во внимание ряд соображений, которые могут накладывать ограничения на использование перемещаемых профилей:

- **Место на диске.** Операционные системы семейства Windows по умолчанию сконфигурированы так, что по завершении сеанса работы пользователя все данные его профиля остаются на локальном компьютере. Значит, нужно обращать внимание на то, есть ли на локальном диске свободное место, чтобы мог начать работу следующий пользователь.
  Можно избавиться от этого ограничения, если по окончании сеанса удалять из компьютера копию перемещаемого профиля пользователя. Но это не всегда удобно (например, для ноутбуков такое решение неуместно), а кроме того, такое решение создает дополнительную нагрузку на сеть.
- **Нагрузка на сеть.** Частью профиля пользователя является папка «Мои документы». Если пользователи поступают в соответствии с общепринятой в ОС Windows 2000/XP практикой хранения документов именно в этой папке, то размер их профилей может достигать нескольких гигабайт. После перехода на перемещаемые профили такие пользователи окажутся в неприятной ситуации: при первой регистрации на какой-либо рабочей станции весь профиль придется скопировать на нее по сети. Сколько времени это займет? В крупных сетях Ethernet со скоростью 100 Mbps для передачи двух гигабайт потребуется около

получаса. По завершении сеанса работы изменения в папке «Мои документы» (то есть вновь созданные и отредактированные файлы) понадобится скопировать обратно на сервер, что тоже создает нагрузку на сеть.
Решением в этой ситуации будет еще одна возможность Windows 2000/XP: переадресация папок, о которой мы скажем далее.

- **Конфигурация рабочих станций.** Для успешного использования перемещаемых профилей все компьютеры, на которых будет работать один и тот же пользователь, должны иметь примерно одинаковую конфигурацию аппаратного и программного обеспечения (одинаковое разбиение жесткого диска на разделы, примерно равный размер разделов, одно и то же место хранения локальных профилей, одинаковый набор установленных приложений и пакетов обновления и т.п.).

13.5.1. Правила

Для оптимизации использования перемещаемых профилей рекомендуется придерживаться нескольких несложных правил.

Запретите регистрацию на рабочих станциях до запуска сетевых служб

Возможность регистрации в домене без сети впервые появилась в системе Windows XP Professional. По умолчанию эта возможность разрешена. В таком случае пользователь с перемещаемым профилем при регистрации загружает копию профиля из локального кэша. Это значит, что при переходе на перемещаемые профили с локальных изменения вступают в силу только со второго сеанса работы.

В главе 7 мы отключили эту возможность, и все действия, описанные до сих пор в настоящей главе, выполнялись в то время, пока она оставалась отключенной. Если вы ее в свое время не отключили, то найти ее можно в объекте групповой политики Default Domain Policy, в ветви **Конфигурация компьютера\Административные шаблоны\Система\Регистрация.** Это настройка **При включении компьютера и входе пользователя всегда дожидаться ответа сети (Always wait for the network at computer startup and logon).**

Избегайте использования перемещаемых профилей в неоднородной сети

Если же на ваших рабочих станциях работают как ОС Windows 2000, так и Windows XP Professional, а перемещаемые профили почему-либо необходимы, то руководствуйтесь следующими правилами:

- Операционные системы должны быть установлены в одноименных папках и в одних и тех же разделах.
- В обеих системах должны быть установлены одинаковые версии приложений.
- Приложения должны быть установлены в одноименных папках в одних и тех же разделах.

Обеспечьте доступ администраторов к профилям пользователей

Доступ к профилям пользователей необходим с точки зрения управления сетью. Если это возможно, обеспечьте его ещё до начала работы пользователей.

Исключите папку «Мои документы» из перемещаемого профиля

Переадресацией папки «Мои документы» и исключением ее из профиля вы добьетесь того, что при первой регистрации пользователя на конкретной рабочей станции все содержимое этой папки не будет копироваться по сети на эту рабочую станцию. Таким образом регистрация пройдет быстрее и без лишней нагрузки на сеть. О переадресации папок будет сказано далее.

Не шифруйте файлы в перемещаемых профилях

Применение шифрующей файловой системы (EFS) несовместимо с перемещаемыми профилями. Если вы зашифруете файлы или папки, профиль потеряет способность к перемещению.

13.5.2. Профиль по умолчанию

Когда пользователь впервые приступает к работе, профиль для него создается операционной системой из некоторого шаблона. Этот шаблон может не соответствовать требованиям предприятия, а просить пользователей настроить свой профиль самостоятельно не всегда позволяет их квалификация. Решением будет предварительная настройка шаблона силами администратора. Возможность последующих изменений профиля самим пользователем можно отрегулировать с помощью групповой политики.

В параграфе 13.3 уже было сказано, что при первой регистрации пользователя на компьютере, где у него еще нет профиля, операционная система начинает поиск шаблона профиля с папки `NETLOGON\Default User` на контроллере домена. Это относится как к перемещаемым профилям, так и к локальным. Значит, администратору легко настроить шаблон для профилей обоих типов.

Создание шаблона

Для создания шаблона проделайте следующее:

1. Выберите пользователя, для которого еще не существует никакого профиля (иначе содержимое, например, его папки «Мои документы» станет частью шаблона — а вам это нужно?). Зарегистрируйтесь на PC001 под его именем. Пусть для определенности это будет пользователь `Marketing1`.
2. Настройте свой профиль. Для наглядности внесите следующие изменения:
   - Переключите главное меню на классический вид (щелкните правой кнопкой мыши по кнопке **Пуск**, выберите команду **Свойства** и установите переключатель в положение **Классическое меню**).
   - Смените фоновый рисунок рабочего стола (щелкните правой кнопкой мыши на рабочем столе, выберите команду **Свойства**, перейдите на вкладку **Рабочий стол**, выберите рисунок из списка и нажмите **ОК**).
   - Создайте на рабочем столе документ под названием «Срочно прочитайте» и разместите его значок примерно посередине рабочего стола.
   - В папке «Мои документы» создайте подпапку «Правила для новых сотрудников». На реальном предприятии именно так быстрее всего провести инструктаж нового работника.
3. Закончите сеанс работы.

Копирование шаблона на сервер

Копирование шаблона на сервер осуществляется следующим образом:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Создайте в папке `WINDOWS\SYSVOL\sysvol\study.local\scripts` подпапку «Default User».
3. Выполните команду **Пуск** → **Выполнить** и в поле **Открыть** введите путь `\\PC001\C$`. Отобразится содержимое диска C: компьютера PC001. Перейдите в папку «Documents and Settings\Marketing1».
4. В окне Проводника включите режим отображения скрытых файлов, чтобы увидеть профиль полностью.
5. Скопируйте содержимое папки «Marketing1» в подпапку «Default User» на сервере. Процесс копирования должен занять не больше нескольких секунд.

Примечание.

Перемещаемые профили можно хранить на рядовом сервере, но шаблон профиля (папка «Default User») обязательно должен располагаться на контроллере домена.

Если в вашей сети несколько контроллеров домена, то следует подождать, пока завершится репликация базы данных, потому что папка «Default User» должна присутствовать на любом контроллере, через который регистрируется пользователь, а определить заранее, какой это будет, невозможно.

Проверка функциональности шаблона

Для проверки функциональности шаблона выполните следующие действия:

1. Выберите пользователя, для которого вы определили в свойствах учетной записи, но еще не создали перемещаемого профиля (например, `Shop3`). Если вы поторопились и создали профили для всех, то можете удалить соответствующую папку профиля из папки `C:\TravProfiles` на сервере, а затем уничтожить ее локальную копию на той рабочей станции, за которой собираетесь проверять шаблон. Зарегистрируйтесь на этой рабочей станции под именем `Shop3`.
2. Убедитесь, что настройки, выполненные вами от имени пользователя Marketing1 и затем скопированные на контроллер домена в качестве шаблона, действительны для пользователя `Shop3`.
3. Откройте окно свойств системы, перейдите на вкладку **Дополнительно** и, нажав на кнопку **Параметры** в части **Профили пользователей**, убедитесь, что ваш профиль действительно перемещаемый.
4. Теперь выберите пользователя, для которого определен, но еще не создан, локальный профиль (например, `Manager1`). Зарегистрируйтесь под его именем и убедитесь, что его локальный профиль тоже создан на основе шаблона `Marketing1`.

Таким образом, настройка шаблона на контроллере домена является универсальным системным решением, с помощью которого легко раз и навсегда определить, как будет выглядеть рабочая среда нового пользователя независимо от того, перемещаемый ли у него профиль или локальный.

Гораздо худшим решением было бы создавать шаблон на каждой рабочей станции в папке `%SYSTEMDRIVE%\Documents and Settings\Default User` (из параграфа 13.3 вы знаете, что здесь операционная система ищет шаблон на следующем шаге). Это ненамного уменьшит нагрузку на сеть, но намного прибавит работы администраторам, особенно если количество пользователей сети исчисляется сотнями.

13.5.3. Обязательный профиль

Профиль пользователя недолго останется неизменным. Кто-то поместит на рабочий стол ярлык самой нужной папки, кто-то сменит хранитель

экрана, и все без исключения начнут заполнять папку «Мои документы». Возникает вопрос, все ли такие изменения допустимы правилами предприятия и желательны для администратора. Ведь бесконтрольные изменения могут довести размер профиля до нескольких гигабайт (даже если исключить из него папку «Мои документы», пользователь сможет держать объемистые файлы непосредственно на рабочем столе), которые нежелательно гонять туда-сюда по сети.

Любой администратор предпочел бы, чтобы только некоторые параметры профиля допускали настройку самим пользователем, а все остальные оставались неизменными. Такая возможность существует начиная с Windows NT 4.0 и называется обязательным профилем.

В обязательном профиле изменения, вносимые пользователем, не сохраняются.

Чтобы сделать профиль пользователя `Shop3` обязательным, переименуйте в папке профиля на сервере (C:\TravProfiles\Shop3) файл NTUSER.DAT в NTUSER.MAN.

Теперь, если вы, зарегистрировавшись под именем `Shop3` на PC001, смените, например, фоновый рисунок рабочего стола, то во время следующего сеанса работы пользователь `Shop3` все равно увидит старый вариант.

Примечание.

У файла NTUSER.DAT обычно установлен атрибут «скрытый». Чтобы увидеть его, включите в свойствах папки отображение скрытых файлов.

Изменение расширений не является системным решением. Этот способ превращения профиля в обязательный пригоден только для перемещаемого профиля, который хранится на сервере. Для пользователей с локальными профилями администратору пришлось бы менять расширение файла NTUSER.DAT на каждой рабочей станции, что слишком трудоемко.

Кроме того, этот способ применим только к уже существующим профилям. Если вы измените расширение в папке `Default User` на контроллере домена, то шаблонный профиль для новых пользователей не сработает должным образом.

Системным решением в этом случае будет применение групповой политики. Если на клиентских компьютерах установлена ОС Windows XP Professional, то вы можете включить политику **Запретить перенос изменений в перемещаемых профилях на сервер**, которая находится в ветви **Конфигурация компьютера\Административные шаблоны\Система\Профили пользователей.** В ОС Windows 2000 этот способ неприменим.

Рекомендуется избегать использования обязательных профилей везде, где это только возможно, отключая отдельные возможности настройки при помощи групповых политик. Например, если вы хотите всего лишь, чтобы пользователи не помещали на рабочий стол посторонних изображений в качестве обоев, то примените политику **Скрыть вкладку «Рабочий стол»**.

Дальнейшие сведения о групповых политиках вы найдете в 17 главе.

13.5.4. Домашние папки

Домашние папки и их создание

Изменения в обязательном профиле имеет право производить только член группы администраторов. Но по умолчанию в профиль входит папка «Мои документы». Если вы смените тип профиля на обязательный, то эта папка окажется пользователю недоступной. Ему придется сохранять личные документы где-либо вне профиля, что нежелательно как с точки зрения безопасности (к этой папке могут получить доступ другие), так и с точки зрения мобильности пользователя в пределах сети и удобства резервного копирования, поскольку эта папка скорее всего будет располагаться на локальном компьютере.

Способом устранить второе неудобство является использование домашних папок.

Домашняя папка — это папка на сервере, предназначенная для хранения личных документов пользователя. Она доступна с любого компьютера сети, но при этом не входит в профиль, не влияет на его размер и не подчиняется групповым политикам, управляющим профилем.

В нашей сети домашние папки пользователей будут размещены на сервере SRVR001 в папке `C:\HomeFolder`. Откройте сетевой доступ к этой папке и предоставьте право «Полный доступ» группе «Зарегистрированные пользователи» («Authenticated Users»).

Чтобы создать домашнюю папку для пользователя `%username%`, выполните следующие действия:

1. Запустите на сервере SRVR001 консоль **Active Directory — пользователи и компьютеры** и отобразите свойства учётной записи, в которой вы хотите поместить домашнюю папку.
2. На вкладке **Профиль** в части **Домашняя папка** установите флажок **Подключить**, оставьте обозначение диска Z: и в поле **к:** введите адрес: `\\SRVR001\HomeFolder\%username%`. Нажмите **OK**. На вопрос, хотите ли вы предоставить пользователю полный доступ к его папке, ответьте **Да**.

Безопасность домашней папки

В ОС Windows Server 2000 разрешения NTFS на домашнюю папку автоматически настраивались правильно, но в Windows Server 2003 этого почему-то не происходит (проверено в версии Beta 2). Администратору придется поработать дополнительно.

На сервере SRVR001 откройте окно свойств только что созданной домашней папки и перейдите на вкладку **Безопасность**. Вы видите, что в списке субъектов доступа присутствует группа «Пользователи» с разрешением создавать подпапки и файлы в данной папке. С точки зрения безопасности это нежелательно.

Удалите группу «Пользователи» из списка субъектов доступа нажатием на кнопку **Удалить**. Вместо нее добавьте учетную запись пользователя, для которого предназначена эта папка, с разрешением «Полный доступ». Предоставьте полный доступ также группе администраторов домена (в случае рядового сервера — группе локальных администраторов).

13.6. Дальнейшие настройки профиля

Когда пользователь с перемещаемым профилем завершает сеанс работы, остается ли профиль в памяти компьютера? Не займет ли он слишком много места на диске? А если удалить его, то сможет ли пользователь впоследствии зарегистрироваться на этом компьютере в отсутствие подключения к сети? Эти и другие характеристики профиля можно настроить при помощи групповых политик из раздела **Конфигурация компьютера\Административные шаблоны\Система\Профили пользователей.**

Удаление профиля по завершении работы пользователя

Эта политика предназначена для тех условий, когда на локальном диске недостаточно места или на компьютере опасно оставлять конфиденциальную информацию пользователей. Включите параметр **Удалять копии перемещаемых профилей из памяти**.

Недостатком этой политики является невозможность открыть свой профиль в случае, когда компьютер не подключён к сети или контроллер домена недоступен. Кроме того, в начале каждого сеанса работы весь профиль будет копироваться по сети заново, что создаст дополнительную нагрузку на сеть.

Запрет перемещаемых профилей

Это политика **Разрешить только локальные профили**. Если данная политика включена, то, когда пользователь с перемещаемым профилем впервые начнёт работу, его профиль не будет скопирован из сети, а вместо этого будет создан новый локальный профиль, который останется в компьютере после окончания пользователем сеанса работы. Таким образом, эта политика подходит для компьютеров, в которых следует обеспечить как можно более быструю регистрацию независимо от состояния сети. Удобна она и для администратора, позволяя ему проверить, регистрировался ли и когда именно тот или иной пользователь на данном компьютере.

Ограничение объёма профиля

Это политика **Ограничить объём профиля**. Она полезна вообще (с точки зрения ограничения нагрузки на сеть), но особенно — для того компьютера, за которым может работать много пользователей, чьи профили могут быстро заполнить весь его жесткий диск.

Если эта политика включена, то при достижении профилем порога допустимого размера пользователю будет показано предупреждающее сообщение и завершение сеанса работы станет невозможно, пока пользователь не уменьшит объем своего профиля. Данную политику обязательно применять вместе с настройкой домашней папки, чтобы пользователь мог перенести личные документы из папки «Мои документы», входящей в профиль, в эту папку.

13.7. Итоги

В системах семейства Windows NT/2000/XP каждый пользователь имеет свой профиль, содержащий его индивидуальные настройки рабочей среды, приложений и, по умолчанию, личные документы. Другим пользователям этот профиль недоступен.

При регистрации пользователя операционная система проверяет в системном реестре, существует ли уже профиль данного пользователя на этом компьютере. Если да, то он применяется, если нет, то создается новый. По завершении сеанса работы изменения, внесённые пользователем, становятся частью профиля и применяются при следующей регистрации.

Чтобы новые профили выглядели одинаково, нужно создать шаблон профиля в папке «Default User» в сетевой папке NETLOGON на контроллере домена.

Пользователям, работающим за разными компьютерами, пригодится перемещаемый профиль, который хранится на сервере, а применяется на любой рабочей станции, на которой регистрируется этот пользователь, обеспечивая таким образом одинаковую рабочую среду и доступ к одним и тем же личным документам. Недостатком перемещаемых профилей является повышенная нагрузка на сеть.

Когда пользователь впервые регистрируется на некотором компьютере, весь профиль копируется в этот компьютер с сервера. Пока профиль не скопировался полностью, пользователь не может начать работу.

Чтобы запретить пользователям вносить изменения в стандартный профиль, вы можете сделать их профили обязательными, переименовав файл NTUSER.DAT в NTUSER.MAN. Запретить только некоторые изменения можно с помощью групповых политик.

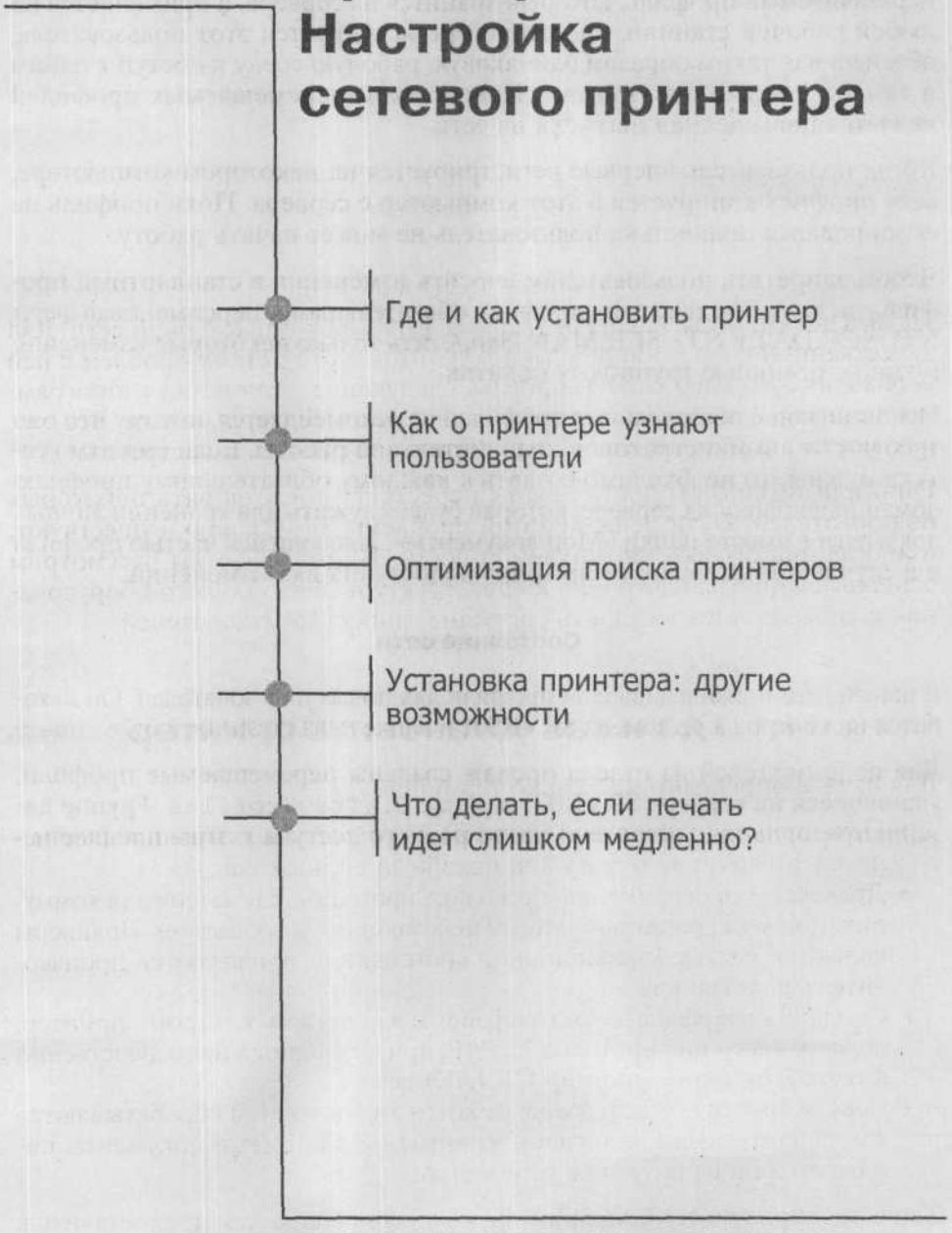
Использование обязательных профилей не рекомендуется, потому что они требуют от администраторов дополнительной работы. Если они вам все-таки нужны, то необходимо создать к каждому обязательному профилю домашнюю папку на сервере, которая будет служить для хранения личных документов вместо папки «Мои документы», являющейся частью профиля и в случае обязательности профиля недоступна для изменений.

Состояние сети

В нашей сети появился шаблон профиля для новых пользователей. Он находится на контроллере домена SRVR001 в папке `NETLOGON\Default User`.

Для пользователей из отдела продаж созданы перемещаемые профили, хранящиеся на сервере SRVR001 в папке `C:\TravProfiles`. Группе администраторов предоставлено право полного доступа к этим профилям.

Глава 14 Принтер в сети. Настройка сетевого принтера



Печать документов — одна из главных функций компьютерной сети. Для качественной и быстрой печати документов и отсутствия проблем с ней необходимо хорошо отрегулировать следующие устройства и программы: принтеры, интерфейс для их подключения, серверы печати. Все это, разумеется, необходимо должным образом соединить и настроить.

Рано или поздно скорость печати перестает удовлетворять некоторых пользователей. Пути решения этой проблемы, безусловно, существуют, и иногда они бывают неожиданно просты. В этой главе мы рассмотрим основные вопросы настройки инфраструктуры печатающего оборудования и способы удовлетворить растущие запросы пользователей.

14.1. Где и как установить принтер

Для начала определим несколько терминов.

- Печатающее устройство (принтер) — устройство, выполняющее печать напрямую на бумагу или подобный ей носитель.
- Драйвер — программа или несколько программ, служащих для коммуникации между компьютером и печатающим устройством. Драйверы являются частью операционной системы или прилагаются производителями устройств.
- Сетевой интерфейс — интерфейс, посредством которого принтер, поддерживающий протокол TCP/IP, присоединяется непосредственно к сети. Пример — принтер HP JetDirect.
- Сервер печати — компьютер, на котором документы обрабатываются для печати, задается порядок их печати и с которого документы посылаются на печатающее устройство.

Наше предприятие купило принтер, который собирается предоставить в распоряжение всех пользователей (в дальнейших примерах будем считать, что это принтер LaserJet 2100). Кроме этого, к серверу подключен принтер HP DeskJet 690C, который для пользователей не предназначен.

14.1.1. Способы подключения принтеров

Большинство принтеров можно присоединить к компьютеру через порт USB или параллельный порт (LPT), но это решение пригодно только в домашних условиях, когда у пользователя рядом стоят единственный компьютер и единственный принтер. В локальной сети предприятия удобнее использовать принтеры, подключаемые непосредственно к сети.

14.1.2. Установка струйного принтера для обслуживания сервера

Методика установки струйного принтера в данном случае выглядит следующим образом:

1. Зарегистрируйтесь на SRVR001 как администратор. Откройте окно **Пуск → Принтеры и факсы**. Выберите из панели задач печати задачу **Установка принтера**.
2. Запустится Мастер установки принтера. Нажмите кнопку **Далее**. В следующем окне выберите **Локальный принтер, подключенный к этому компьютеру** и снимите флажок **Автоматическое определение и установка принтера «Plug and Play»**.
3. В диалоговом окне **Выбрать порт принтера** оставьте исходное значение (рис. 14.1) и нажмите **Далее**.
4. В диалоговом окне **Установить программное обеспечение принтера** выберите из списка **Изготовитель** пункт HP, а из списка **Принтеры** пункт HP DeskJet 690C. Нажмите **Далее**.
5. В диалоговом окне **Название принтера** оставьте слова HP DeskJet 690C и нажмите **Далее**.

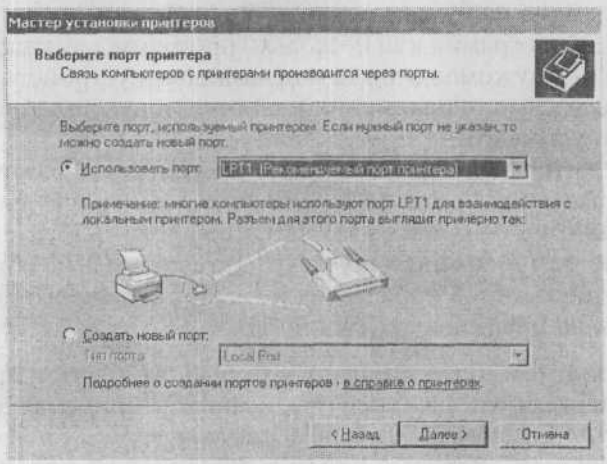


Рис. 14.1. *Принтер будет установлен на порт LPT1*

6. В окне **Использование общих принтеров** выберите пункт **Нет общего доступа к этому принтеру**. Принтер предназначен только для сервера, поэтому нет необходимости открывать к нему сетевой доступ.
7. В диалоговом окне **Напечатать пробную страницу** выберите пункт **да** или **нет** в зависимости от того, есть ли у вас сейчас возможность напечатать страницу, нажмите **Далее** и завершите работу мастера нажатием кнопки **Готово**.

Значок установленного принтера появится в папке «Принтеры и факсы».

14.1.3. Установка лазерного принтера для обслуживания пользователей

Чтобы подключить принтер HP LaserJet 2100 к сети, вам придется дополнительно купить сетевую карту HP JetDirect и установить для него собственный IP-адрес, который можно задать при помощи программы, прилагаемой к принтеру, либо получить от сервера DHCP. Более подробную информацию вы найдете в инструкции или руководстве к принтеру.

IP-адрес принтера должен быть всегда одним и тем же, поэтому, если вы собираетесь арендовать адрес в службе DHCP, то это должен быть зарезервированный IP-адрес. Другим решением была бы статическая адресация, выгодная тем, что позволяет избежать проблем, связанных с недоступностью сервера DHCP.

Резервирование адреса

В главе 3 мы отвели для принтеров и других сетевых устройств диапазон адресов от 192.168.10.12 до 192.168.10.16. Назначим данному принтеру первый адрес из этого диапазона. Нам понадобится еще один параметр — физический MAC-адрес сетевой карты HP JetDirect. В инструкции пользователя должно быть написано, как можно его определить.

1. Зарегистрируйтесь на SRVR001 как администратор. Откройте консоль DHCP.
2. В окне консоли раскройте контейнер srvr001.study.local [192.168.10.2], а затем область [192.168.10.0] Main Office.
3. Правой кнопкой мыши щелкните по значку **Резервирование** и из контекстного меню выберите команду **Создать резервирование**.
4. В диалоговом окне **Создать резервирование** введите название принтера, в поле **IP-адрес** введите 192.168.10.12, а в поле **MAC-адрес** — физический адрес сетевой карты. Остальным параметрам оставьте исходные значения и нажмите кнопку **Добавить**.

Рис. 14.2. *Резервирование IP-адреса на сервере DHCP*

После этого нужно подключить принтер к сети и включить его. Его IP-адрес (независимо от того, получен ли он на сервере DHCP или установлен программой, прилагаемой к принтеру) активизируется.

Установка принтера

Установка принтера состоит из следующих этпаов:

1. Зарегистрируйтесь на SRVR001 как администратор. Откройте окно **Пуск → Принтеры и факсы**. Выберите из панели задач печати задачу **Установка принтера**.
2. Запустится Мастер установки принтера. Нажмите кнопку **Далее**. В следующем окне выберите **Локальный принтер, подключенный к этому компьютеру** и снимите флажок **Автоматическое определение и установка принтера «Plug and Play»**. Нажмите **Далее**.

Примечание.

На первый взгляд может показаться, что надо было выбрать вариант **Сетевой принтер**, но мы собираемся сделать SRVR001 сервером печати.

3. В диалоговом окне **Выберите порт принтера** поставьте переключатель в положение **Создать новый порт** и выберите из списка **Стандартный порт TCP/IP**. Нажмите **Далее**. Запустится Мастер добавления стандартного TCP/IP-порта принтера.
4. Пока новый принтер не прописан в службе DNS, он идентифицируется только по IP-адресу: введите в поле **Имя принтера или IP-адрес** назначенный адрес 192.168.10.12. Нажмите **Далее**.

5. В диалоговом окне **Требуются дополнительные сведения о порте** выберите пункт «Hewlett Packard Jet Direct» и нажмите кнопку **Далее**. Еще раз проверьте заданные параметры и нажмите **Готово**.
6. В диалоговом окне **Установить программное обеспечение принтера** выберите из списка **Изготовитель** пункт HP, а из списка **Принтеры** — пункт HP LaserJet 2100.
7. В диалоговом окне **Имя принтера** оставьте имя по умолчанию (HP LaserJet 2100), в нижней части окна выберите ответ **Да**.
8. В диалоговом окне **Использование общих принтеров** выберите **Нет общего доступа к этому принтеру**. Мы откроем общий доступ позже.
9. Далее можете напечатать или отказаться от печати пробной страницы и завершите работу Мастера нажатием кнопки **Готово**.

14.1.4. Настройка сервера печати

Установкой принтеров мы добавили к списку ролей компьютера SRVR001 еще одну роль — сервера печати. Теперь именно на этом компьютере задания на печать будут ставиться в две очереди, и только он будет непосредственно связываться с двумя принтерами.

Настройка сервера печати не зависит от количества или типа установленных принтеров.

Зарегистрируйтесь на SRVR001 как администратор. Откройте окно **Пуск → Принтеры и факсы**. Выберите из строки меню команду **Файл → Свойства сервера** (рис.14.3).

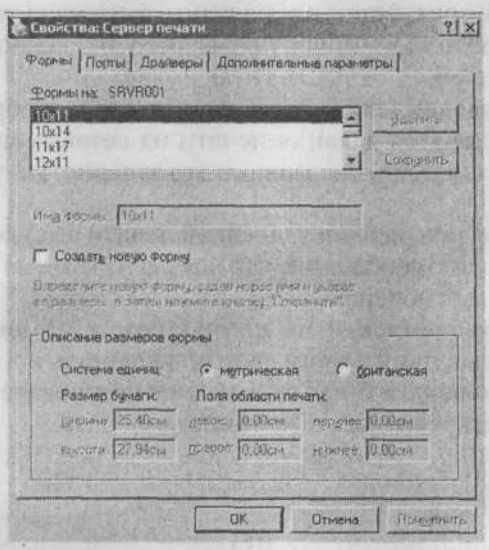


Рис. 14.3. *Диалоговое окно свойств сервера печати*

Самые важные для управления принтерами параметры находятся на вкладке **Дополнительные параметры**. Здесь можно настроить следующее:

- **Папка очереди печати**: это папка на жестком диске компьютера, в которую помещаются задания печати для всех принтеров и происходит их обработка. С точки зрения надежности выгоднее размещать эту папку не на том диске, на который установлена операционная система. На этом диске должно быть достаточно места, потому что нехватка места в процессе печати может вызвать сбой печати.
  Смена этой папки будет осуществлена сразу после того, как вы нажмете кнопку **OK**. Если в папке в этот момент были какие-то задания, ожидающие выполнения, то их печать будет отменена. Это значит, что смену папки следует проводить в то время, когда в очереди нет текущих заданий.
- **Вести журнал ошибок очереди печати, Вести журнал предупреждений очереди печати, Вести журнал сообщений очереди печати**: флажки, отвечающие за то, какие именно события печати будут отражены в протоколе приложения. Этот протокол можно просмотреть в окне консоли **Администрирование → Просмотр событий.** По умолчанию протоколирование включено.
- **Звуковой сигнал при ошибках удаленной печати документов**: эта функция полезна лишь в том случае, если сервер находится в «радиусе слышимости» администраторов, в противном случае сигнал никто не услышит. По умолчанию звуковой сигнал выключен.
- **Показывать уведомления локальных принтеров**: если этот флажок установлен, то состояние, в котором находятся задания печати на локальных принтерах, будет отображено в форме контекстной подсказки на компьютере пользователя, пославшего это задание. По умолчанию режим выключен.
- **Показывать уведомления сетевых принтеров**: отображать состояние, в котором находятся задания печати на сетевых принтерах, на компьютере пользователя, пославшего это задание. По умолчанию режим включен.
- **Уведомление о завершении удаленной печати документов**: пользователю будет отослано сообщение, что документ отпечатан. По умолчанию эта функция выключена.
- **Передавать уведомление на компьютер, а не пользователю**: если включен предыдущий режим, можно включить и этот. В этом случае уведомление о печати будет отослано не пользователю, а компьютеру, с которого документ был отправлен на печать.

14.1.5. Настройка принтеров

Перед тем как предоставить пользователям возможность работать с установленным принтером, необходимо настроить его. Отобразите окно свойств принтера, выбрав команду **Свойства** из контекстного меню значка принтера в окне папки **Принтеры и факсы**. Окно свойств состоит из нескольких вкладок.

- Вкладка **Дополнительно**. Здесь вы можете указать часы, в которые принтер будет доступен для печати. Активируйте пункт «Доступен с ... по ...» и введите время, в которое печать на данном принтере будет возможна. Если пользователь отошлет документ на печать в неуказанное время, то задание будет не отклонено, а поставлено в очередь и напечатано в разрешенное время.
- Вкладка **Безопасность**. Здесь задаются разрешения: отдельно на печать и отдельно на управление документами и управление принтером. По умолчанию разрешение на печать предоставлено группе «Все», а управлять документами пользователь имеет право только собственными. Это значит, что он не может удалить из очереди документ, поставленный туда другим пользователем.
- Вкладка **Доступ**. Здесь вы можете открыть сетевой доступ к принтеру. Установите переключатель в положение **Общий доступ к данному принтеру**, а в поле **Сетевое имя** введите название, под которым принтер будет известен в сети (например, HP2100).

Также убедитесь в том, что установлен флажок **Внести в Active Directory**. Активация этого параметра значит то, что в доменной базе данных Active Directory появится объект сетевого принтера, через который пользователи смогут его найти. Иными словами, активацией этого пункта вы донесете до пользователей информацию о доступности этого принтера для всех пользователей, которым вы предоставили разрешение на печать.

Кнопка **Дополнительные драйверы** позволяет подключить этот принтер в качестве сетевого пользователям, сидящим за компьютерами с операционными системами версий более ранних, чем Windows 2000. Для подключения сетевого принтера к рабочей станции под управлением Windows NT 4.0 нужны драйверы, которых в этой операционной системе нет. Она будет искать их в папке с драйверами на сервере (\\SRVR001\print$), а если не найдет, то потребует установить их с диска. Полномочий на установку драйверов у рядового пользователя нет, значит, эту проблему придется решать вам как администратору.

Нажмите кнопку **Дополнительные драйверы** (рис. 14.4). Для операционной системы Windows NT 4.0 установите флажок **x86** и нажмите **OK**. После этого драйверы принтера HP LaserJet 2100 для системы Windows NT 4.0 будут помещены на сервер печати, откуда система, установленная на компьютере пользователя, автоматически скачает и установит их при первой печати.

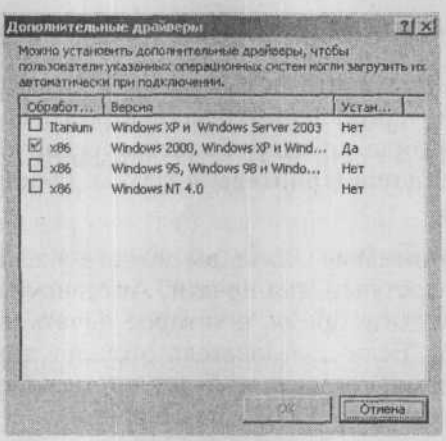


Рис. 14.4. *Установка драйверов принтера для других операционных систем*

Примечание.

Если впоследствии вы обновите драйверы данного принтера для всех операционных систем (в том числе Windows NT 4.0), клиентские операционные системы перед началом следующей печати скачают новые драйверы и также автоматически установят. В системах семейства Windows NT проверка наличия новейшей версии драйвера производится перед печатью каждого документа.

14.1.6. Проверка наличия принтера в активном каталоге

Активацией пункта «Внести в Active Directory» запись о сетевом принтере добавляется в доменную базу данных Active Directory. Необходимо убедиться в том, что она там есть.

Зарегистрируйтесь на SRVR001 как администратор. Запустите консоль **Active Directory — пользователи и компьютеры**.

Раскройте объект **study.local\Контроллеры домена** и щелкните по SRVR-001. В правой части окна консоли отобразится значок сетевого принтера. Изучите свойства этого объекта. Возможно, вы получите некую новую информацию о нем. О том, как и для чего она применяется, пойдет речь ниже.

14.2. Как о принтере узнают пользователи

С тех пор, как на рынок поступила операционная система Windows 2000, корпорация Microsoft изменила политику в области разработки программ поддержки печати. Они стали более практичны и требуют от пользователя меньшей квалификации. Теперь пользователю не нужно узнавать, какой из сетевых принтеров поддерживает цветную печать, чтобы отправить свои фотографии именно на него. Ему вообще не нужно ничего знать о характеристиках принтеров. Операционная система сама выберет принтер, на котором можно отпечатать документ с заказанными параметрами.

Чтобы проверить это утверждение, зарегистрируйтесь на PC001 как рядовой пользователь, запустите Блокнот и напишите несколько строк. Отправьте текстовый документ на печать:

1. Выполните команду **Файл** → **Печать** и откажитесь от установки принтера.
2. В диалоговом окне печати нажмите кнопку **Найти принтер**.
3. В окне **Поиск: Принтеры** перейдите на вкладку **Возможности**. Допустим, вам требуется отпечатать черно-белый документ на листе формата A4 с максимальной скоростью. Из списка **Формат бумаги** выберите A4, в поле **Минимальная скорость печати** введите значение 8 (страниц в минуту) и нажмите **Поиск**. Через некоторое время в нижней части окна появятся результаты поиска: принтер HP LaserJet 2100 поддерживает все характеристики печати, которые нам нужны.
4. Щелкните правой кнопкой мыши по значку найденного принтера и из контекстного меню выберите команду **Подключить**. Нажатием кнопки **OK** закройте диалоговое окно.

Найденный и подключенный таким образом принтер останется в распоряжении пользователя точно так же, как если бы он подключал его самостоятельно.

Теперь хорошо бы узнать, где физически находится отпечатанный документ. Для этой цели среди свойств принтера существует пункт «Размещение», который должен заполнить администратор. Это можно сделать в ходе установки принтера или позже. Информацию о размещении рекомендуется записывать в следующем виде:

`Место/Город/Номер дома/Этаж/Комната`
(например, Центральный офис/Санкт-Петербург/3В/4/412),

где `Место` — это сайт домена Active Directory, то есть подразделение, в котором находится контроллер домена (дальнейшие сведения о понятии «Сайт» вы найдете в главе 27).

1. Зарегистрируйтесь на SRVR001 как администратор. Откройте окно **Пуск → Принтеры и факсы**.
2. Отобразите окно свойств принтера HP LaserJet 2100 и перейдите на вкладку **Общие**.
3. В поле **Размещение** введите описание физического расположения сервера печати и нажмите **OK**.

Теперь в диалоговом окне **Поиск: Принтеры** пользователь сможет просмотреть информацию о размещении найденных принтеров и выбрать для печати ближайший к своему рабочему месту.

Искать принтеры можно не только в диалоговом окне **Печать** какого-либо приложения. Для этого также служит команда **Поиск** в главном меню.

14.3. Оптимизация поиска принтеров

14.3.1. Методика и этапы оптимизации поиска принтеров

Если ваше предприятие целиком расположено в одном здании, то этот параграф можете пропустить. Он посвящен тому, как сделать, чтобы для каждого пользователя поиск принтера возвращал только те принтеры, к которым у пользователя есть физический доступ, то есть расположенные в одном с ним здании.

Если пользователь введет в диалоге поиска принтеров в поле **Место** на вкладке **Принтеры** название «Центральный офис», то поиск будет производиться только среди тех принтеров, в свойстве «Размещение» которых присутствует «Центральный офис». Но компьютер пользователя сам находится в центральном офисе, так нельзя ли заполнять это поле автоматически?

Можно. Для этого вам понадобится инструмент, с которым вы еще не работали: консоль **Active Directory — сайты и службы**. С его помощью можно переименовать свой сайт в Central_Office, после чего новое название будет автоматически вноситься в поле **Место** в диалоге поиска. Переименование сайта не имеет значения для его функционирования, его можно рассматривать просто как некую инвентаризацию, проводимую для того, чтобы администратору и пользователям было проще ориентироваться в домене.

1. Зарегистрируйтесь на SRVR001 как администратор и запустите консоль **Пуск → Администрирование → Active Directory — сайты и службы.**

2. В окне консоли, где по умолчанию отображаются только сайты, а службы скрыты, щелкните правой кнопкой мыши по значку «Исходное название первого сайта» и замените название на Central_Office.
3. Щелкните правой кнопкой мыши по значку **Подсети** и из контекстного меню выберите команду **Новая подсеть** (рис. 14.5). Задайте для новой подсети по имени Central_Office адрес и маску, как показано на рисунке, выберите в списке **Имя сайта** Central_Office и нажмите **OK**.

Рис. 14.5. *Диалог задания подсети*

4. Щелкните правой кнопкой мыши по новому объекту подсети и выберите команду **Свойства**.
5. На вкладке **Размещение** введите название Central_Office. Именно это название будет автоматически вводиться в поле **Место** в окне поиска принтеров.
6. Закройте консоль **Active Directory — сайты и службы** и запустите консоль **Active Directory — пользователи и компьютеры**.
7. Вызовите окно свойств домена `study.local`. Перейдите на вкладку **Групповые политики** и выберите объект Default Domain Policy.
8. В консоли **Редактор объектов групповой политики** раскройте объект **Конфигурация компьютера\Административные шаблоны\Принтеры**. В правом окне консоли найдите политику **Pre-populate printer search location text (Заполнение строки поиска принтеров)** (рис. 14.6) и включите ее.

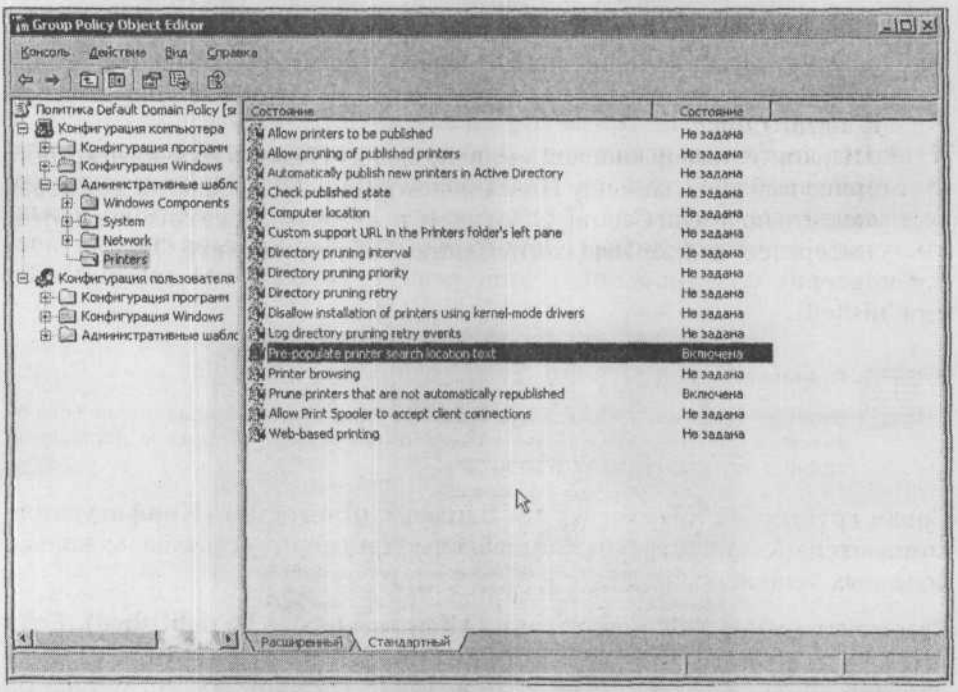


Рис. 14.6. *Групповые политики, относящиеся к принтерам*

Осталось актуализовать настроенные свойства, параметры и политики на всех клиентских компьютерах. Через час-два это будет сделано автоматически. Вручную это можно сделать двумя способами: перезагрузив клиентский компьютер или запустив на нем утилиту командной строки GPUPDATE.

14.3.2. Ограничения на поиск принтеров

Конкретный пользователь сможет найти принтер, только если для этого принтера выполнены следующие условия:

- **К принтеру открыт сетевой доступ.** Мы не открывали доступа к HP DeskJet 690 C, поэтому он при поиске не отображается.
- **Принтер опубликован в активном каталоге.** Если сервер печати работает под управлением ОС Windows 2000/ XP или Windows Server 2003, то подключенный к нему принтер публикуется в базе данных Active Directory автоматически. Если же на нем установлена Windows NT 4.0, то предоставлять принтер в распоряжение пользователей надо вручную.

- **Этому пользователю разрешена печать на этом принтере.** По умолчанию разрешение на печать предоставляется группе «Все». Если вы ограничите доступ другой группой, то пользователи, не входящие в эту группу, не увидят принтера в списке доступных.

Из списка доступных исключаются также те принтеры, чей сервер печати некоторое время не отвечает на запросы контроллера домена (например, этот компьютер выключен). Для того, чтобы этого не происходило, нужно отключить политику **Удалять принтеры, которые не были автоматически повторно опубликованы (Prune printers that are not automatically republished)**.

Примечание.

Этот пункт важен, если в нашей сети больше одного контроллера домена. Если он является единственным и выключен в настоящий момент, то неважно, доступен ли принтер, все равно печать невозможна.

Среди групповых политик, относящихся к принтерам (**Конфигурация компьютера\Административные шаблоны\Принтеры**) есть еще несколько полезных вещей:

Разрешить публикацию принтеров (Allow printers to be published). Если отключить эту политику, то со вкладки **Доступ** диалогового окна свойств принтера исчезнет пункт **Добавить в Active Directory**. Я упоминаю об этой политике не для того, чтобы вы ей пользовались, а чтобы вы знали, где в случае чего искать проблемы.

Проверять состояние публикации (Check published state). Если отключить принтер от сервера печати, то его объект исчезнет из активного каталога не сразу. Служба очистки запускается на контроллере домена по умолчанию каждые 8 часов. Она опрашивает опубликованные принтеры, и если не получит ответа три раза подряд (то есть в течение суток), то удаляет принтер из списка доступных. Интервал опроса можно установить через политику **Directory pruning interval (Интервал очистки Active Directory)**, а количество попыток (до 6) — через политику **Directory pruning retry (Повторы при очистке Active Directory)**.

14.4. Установка принтера: другие возможности

Немногие пользователи знают, что подключенные к сети принтеры, к которым у них есть доступ, они могут инсталлировать на свой компьютер, даже не имея полномочий администратора. Установка при помощи Мастера установки принтеров в этом случае проходит примерно так же, как установка принтера на сервере печати.

1. Зарегистрируйтесь на PC001 как рядовой пользователь.
2. Откройте окно **Пуск → Принтеры и факсы** и выберите задачу **Установка принтера**. Запустится уже знакомый нам Мастер установки принтеров. Нажмите кнопку **Далее**.
3. В диалоговом окне **Локальный или сетевой принтер** убедитесь, что не выбран вариант локального принтера, потому что рядовой пользователь не имеет права устанавливать локальные принтеры.
4. В следующем окне установите переключатель в положение **Обзор принтеров**, если вы уверены, что сможете найти принтер в активном каталоге, а если нет — то в положение **Подключиться к принтеру или выполнить обзор принтеров**. Нажмите **Далее**.
5. Если вы выбрали **Обзор принтеров**, то выполните поиск, как описано в п.14.2, а если другой вариант, то вы должны знать сетевое имя принтера и какой компьютер является для него сервером печати. Вам будут предъявлены все серверы печати, к которым вы как рядовой пользователь имеете доступ. Выберите сервер и принтер и нажмите **Далее**. Для завершения работы Мастера нажмите **Готово**.

Пользователи старой школы подключаются к сетевым принтерам именно так, предварительно выяснив у администратора имена серверов печати и принтеров. А с точки зрения корпорации Microsoft излишние знания для пользователя вредны, и он вполне может довольствоваться автоматическим поиском принтера.

Есть еще немало администраторов, которые думают, что выражение «сетевой принтер» означает принтер, подключенный непосредственно к сети через классический кабель UTP или STP, а не к компьютеру через параллельный порт. Это ошибка. С точки зрения операционной системы, сетевой принтер — это принтер, который локально инсталлирован на какой-нибудь компьютер (сервер печати) и доступен по сети либо непосредственно, либо через этот компьютер. Важно то, что на клиентском компьютере этот принтер всегда нужно устанавливать как сетевой.

Если администратор установит его на некоторую рабочую станцию как локальный (у обычного пользователя нет такого права), он сделает (возможно, сам того не зная) эту рабочую станцию сервером печати. После этого вся обработка задания на печать будет происходить на рабочей станции, отнимая почти все ресурсы центрального процессора. Обычная работа пользователя во время подготовки файла к печати станет невозможна. Если же принтер установлен как сетевой, то обработка задания на печать на рабочей станции сводится к передаче файла по сети на сервер печати.

Обратите внимание, что принтер, установленный пользователем как сетевой, становится частью пользовательского профиля. Если на данной рабочей станции регистрируется другой пользователь, которому тоже нужно печатать, ему придется выбирать и устанавливать сетевой принтер для себя заново.

14.5. Что делать, если печать идет слишком медленно?

На работу в организацию устраиваются новые и новые сотрудники, увеличиваются объемы печати, у серверов печати появляются новые и новые функции и т. д. Причин может быть много, но результат всегда одинаков — недовольство пользователей.

14.5.1. Больше или меньше принтеров?

Что лучше — выделить отдельный дешевый принтер каждому пользователю или поставить один принтер на весь отдел (гораздо более дорогой, но и с лучшими характеристиками)? Сравним эти две возможности с точки зрения администрирования.

Если принтеры будут приобретены для каждого пользователя, то администратору необходимо установить каждый из них как локальный, регистрируясь на каждой рабочей станции под учетной записью администратора. Затем ему придется следить за правильной их работой, осуществлять замену картриджей, вытаскивать застрявшую бумагу и т.д.

Если же выбор был сделан в пользу одного производительного принтера, администратору понадобится только установить его как сетевой и открыть к нему доступ, а подключаться к нему пользователи будут самостоятельно. Один принтер и обслуживать гораздо проще, чем несколько десятков.

На практике вы, весьма вероятно, столкнетесь с ситуацией, когда на один отдел установлен один общий принтер, но приблизительно у 5% пользователей есть еще и собственные принтеры. Если того требуют обстоятельства, то это самое выгодное решение (например, совершенно излишне покупать большой цветной принтер, если распечатать что-нибудь в цвете нужно раз в месяц). У вас будет меньше работы, а предприятие сэкономит на этом.

Все ситуации, когда пользователи недовольны скоростью печати, можно разделить на 2 группы:

- Все пользователи недовольны, так как скорость печати в самом деле *ниже всякой критики*.
- В целом пользователи довольны скоростью печати, но начальство недовольно тем, что приходится ждать, пока очередь дойдет до его документов.

14.5.2. Если недовольны все. Пул принтеров

Самым слабым звеном инфраструктуры печати в крупных организациях являются обычно сами принтеры. Сетевая инфраструктура, емкость и прочие параметры серверов печати обычно в порядке, проблема в том, что сам принтер из-за ограниченности технических возможностей не может отпечатать большего количества страниц в минуту. Обновление драйверов принтера вам не поможет, и вы полагаете, что единственный способ — закупить новые, более совершенные принтеры. Но начальство просит найти более простое и дешевое решение. Такое решение действительно существует.

Если проблема в самом принтере, то, очевидно, вам не придет в голову ничего, кроме его замены или добавления еще одного. Решение, которое в системе Windows носит название «Пул принтеров» (Printer pooling), основано на добавлении нового принтера, точно такого же, как имеющийся, или по крайней мере работающего с тем же самым драйвером (для принтеров компании HP это обычно не проблема).

Добавление принтера в пул является заботой исключительно администратора. Пользователям не нужно подключаться к нему дополнительно; они даже не заметят, что в сети прибавилось принтеров, а почувствуют только, что печать стала быстрее.

Допустим, вы купили еще один принтер HP LaserJet 2100, подключили его к сети с помощью кабеля UTP или STP и назначили ему IP-адрес 192.168.10.13 так, как описано в п.14.1.3. Теперь выполните следующее:

1. Зарегистрируйтесь на SRVR001 как администратор. Откройте окно свойств принтера HP LaserJet 2100 (имеющегося).
2. Перейдите на вкладку **Порты** и нажмите кнопку **Добавить порт**. Выберите из списка «Стандартный порт TCP/IP». Запустится Мастер добавления стандартного TCP/IP порта принтера. Нажмите **Далее**.
3. Введите в поле **Имя принтера или IP-адрес** адрес 192.168.10.13 и нажмите **Далее**.
4. В диалоговом окне **Требуются дополнительные сведения о порте** выберите пункт **Hewlett Packard Jet Direct** и нажмите **Далее**. Для завершения работы Мастера нажмите **Готово**.
5. В диалоговом окне **Завершение мастера добавления стандартного TCP/IP** порта принтера еще раз проверьте заданные параметры и нажмите кнопку **Готово**.
6. Перейдите на вкладку **Доступ** в окне свойств принтера. Вы увидите новый порт 192.168.10.13. В нижней части вкладки установите флажок **Разрешить пул принтеров** и отметьте все порты, к которым подключен принтер (192.168.10.12 и 192.168.10.13). Закройте окно свойств принтера.

Теперь сервер печати будет отправлять документы пользователей на то из двух печатающих устройств, которое менее загружено. При этом каждый файл отправляется целиком на одно устройство, так что пользователю не придется собирать страницы своего документа с разных принтеров.

Физически новое печатающее устройство может быть расположено где угодно в пределах сети, но, поскольку принтер пользователи видят только один и ориентируются на его свойство «Размещение», имеет смысл поставить новое устройство рядом со старым или во всяком случае в том же здании.

14.5.3. Если недовольна только часть пользователей. Назначение и настройка приоритетов печати

Если недовольна лишь часть пользователей, то ситуацию можно разрешить еще более простым способом (без необходимости докупать и устанавливать какое-либо оборудование). Речь идет о том, чтобы предоставить приоритетные права на печать недовольной группе, то есть сделать так, чтобы каждый документ от этой группы ставился в очередь на первое место. Для этого понадобится настроить сетевые принтеры на компьютерах привилегированной группы.

Установка приоритетов печати на сервере

На время настройки приоритета нужно отключить использование пула принтеров и второго IP-адреса.

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Создайте локальную доменную группу безопасности под названием D Print HP LJ 2100 Priority. В эту группу включите недовольных пользователей.
3. Откройте окно **Принтеры и факсы** и установите еще один локальный принтер HP LaserJet 2100 на тот же порт, что и имеющийся принтер (у вас окажется два принтера на одном порту). Оставьте новому принтеру тот же драйвер, а имя дайте «HP LaserJet 2100 Priority».
4. Откройте сетевой доступ к новому принтеру под именем HP2100P.
5. Откройте окно свойств нового принтера и перейдите на вкладку **Безопасность**. Из списка субъектов доступа удалите группу «Все» и добавьте группу «D Print HP LJ 2100 Priority» с разрешением на печать. Затем в перейдите на вкладку **Дополнительно** и в поле **Приоритет** введите значение 10. Закройте диалоговое окно нажатием кнопки **ОК**.
6. Откройте диалоговое окно свойств принтера HP LJ 2100 (старого) и перейдите на вкладку **Безопасность**. В список субъектов доступа добавьте группу «D Print HP LJ 2100 Priority» и запретите ей все действия.

Подготовка сервера завершена, осталось лишь внести изменения на компьютерах пользователей привилегированной группы.

Настройка клиентских компьютеров

При следующей регистрации каждый из пожаловавшихся пользователей окажется членом группы «D Print HP LJ 2100 Priority», которой запрещена печать на старом принтере. Значит, старый принтер они должны будут из своего профиля удалить, а новый установить. Если они запустят поиск принтеров в активном каталоге, то найдут только новый «HP LaserJet 2100 Priority».

14.6. Итоги

Если вам нужно управлять печатью максимально эффективно, то самым логичным решением было бы установить принтер с высокими технологическими характеристиками с подключением к сети с помощью сетевого кабеля UTP/STP. Далее нужно выбрать компьютер — сервер печати, на который этот принтер инсталлируется как локальный. Установка этого принтера как сетевого на другие компьютеры — это работа пользователей, на которую они имеют право. Установленный сетевой принтер становится частью профиля пользователя.

Когда пользователь отправляет документ на сетевой принтер, подготовка документа к печати происходит на сервере печати, не загружая рабочую станцию пользователя.

Принтеры, подключаемые к серверам печати под управлением ОС Windows 2000 и более новых, автоматически прописываются в активном каталоге. Пользователь может найти в активном каталоге принтер, отвечающий его требованиям к характеристикам печати (возможность цветной печати, разрешение, скорость и т. п.). Поиск проводится только среди тех принтеров, к которым у этого пользователя есть доступ на печать. По умолчанию разрешение на печать предоставляется группе «Все».

Если у вас возникли сложности со скоростью печати, у вас в распоряжении два способа избавиться от них. Если жалуются все пользователи, то скорее всего мы имеем дело с проблемой нехватки ресурсов принтера. Вы можете подключить еще один точно такой же принтер, объединив их в пул. Если же на скорость печати жалуется только какая-то группа пользователей, то вы можете установить для нее другой принтер (что будет всего лишь иной формой логической интерпретации все того же печатного устройства), печать на котором будет выполняться в приоритетном режиме.

Компьютер, который производит обработку заданий печати, называется сервером печати. Очередь заданий по печати формируется на его жестком диске. По завершении печати файлы очереди печати автоматически удаляются с диска. Папку очереди желательно размещать не на системном диске.

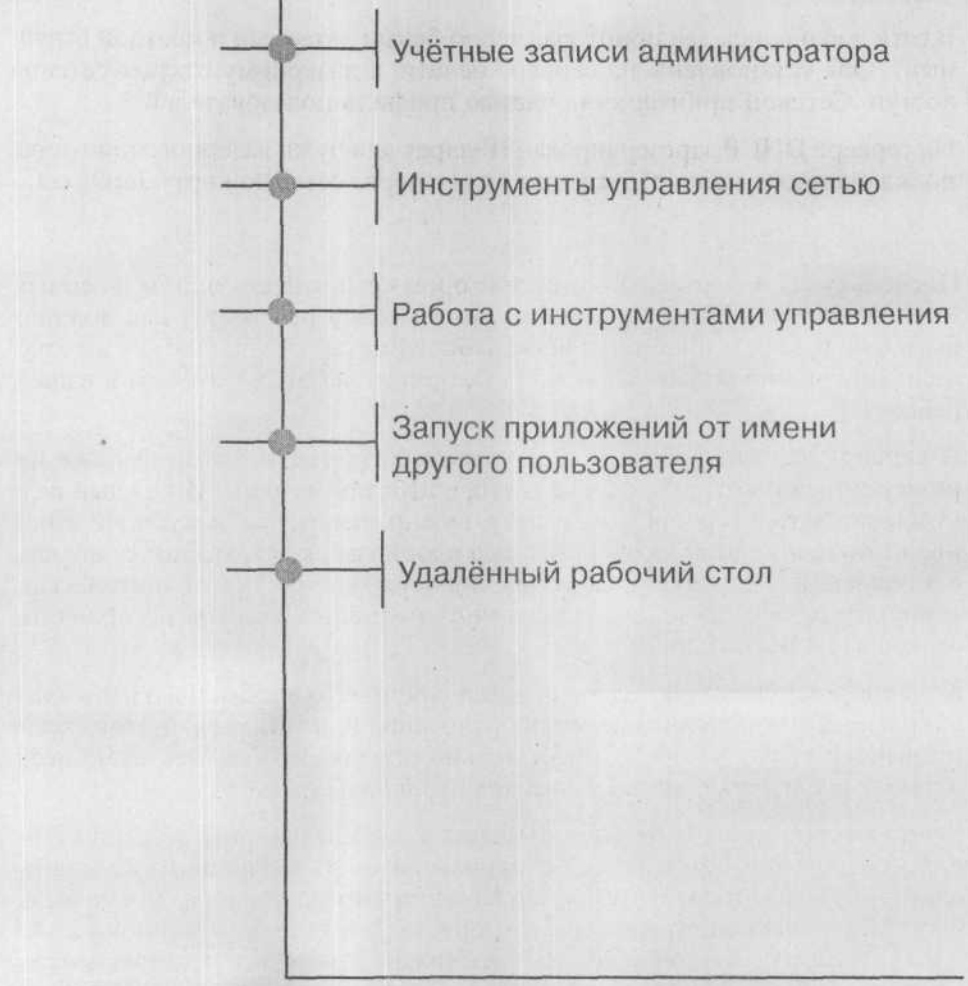
Еще одна функция сервера печати, полезная пользователям, это уведомление о завершении печати. По умолчанию она отключена.

Состояние сети

В сети добавились два принтера (черно-белый лазерный и цветной струйный). Оба установлены на сервере печати, к лазерному открыт сетевой доступ. Сетевой принтер стал частью профиля пользователей.

На сервере DHCP зарезервирован IP-адрес для нужд лазерного принтера, подключенного непосредственно к сети через сетевую карту JetDirect.

Глава 15 Должен ли администратор постоянно сидеть рядом с сервером?



Поскольку вы являетесь администратором сети, то есть одним из самых важных сотрудников предприятия, то ко всему прочему у вас должно быть ещё и просторное и удобное рабочее место. А где ещё бы вы хранили тонны дисков CD-ROM и DVD, просто необходимых вам в вашей работе?

А серверы стоят в какой-нибудь тесной каморке, в которой даже не развернуться и которая, скорее всего, ещё и под замком. И каждый раз, чтобы попасть в серверную комнату, нужно отметиться в журнале охраны, взять ключ, а на десерт, согласно правилам эксплуатации серверов, в помещении вас ожидает заботливо поддерживаемая почти арктическая температура. Не легче ли отказаться от подобных визитов и управлять сервером на расстоянии?

Конечно же, существуют случаи, когда вам просто необходимо быть там: например, подключение нового оборудования или установка нового программного обеспечения, которую нужно производить на месте. Во всех остальных случаях подобных визитов лучше избегать.

Компьютерной сетью можно управлять с любой рабочей станции. Инструменты, с помощью которых производится управление отдельными службами или доменом Active Directory прямо на сервере, могут быть установлены на клиентском компьютере под управлением Windows 2000/XP Professional. В этой главе мы расскажем о порядке установки этих утилит и работы с ними. Но вначале — несколько важных пояснений касательно учётных записей, под которыми можно управлять сетью.

15.1. Учётные записи администратора

15.1.1. Учетная запись рядового пользователя

Для безопасной работы сети следовало бы завести две администраторских записи, причём ни одна из них не должна называться Administrator.

Одна из них предназначена для обычной работы администратора и должна соответствовать полномочиям рядового пользователя. Администратор ведь не только управляет сетью, но и читает почту, запускает браузер Internet Explorer и другие приложения. С полномочиями администратора домена этим заниматься опасно. Например, вы, зарегистрировавшись как администратор, запустили браузер и зашли на страницу, для правильного отображения которой требуется наличие элемента Active X. Решение о том, загружать его или нет, вы принимаете самостоятельно, но от него будет зависеть многое, а именно безопасность и работоспособность сети. Т. к. вы зарегистрированы как администратор, это дает полномочия не только вам, но и программам и скриптам, запущенным вами. И вредоносный код может беспрепятственно поразить не только ваш компьютер, но также и другие в сети.

15.1.2. Учётная запись для текущих административных работ

Эта запись должна обладать полномочиями администратора домена, и текущие настройки нужно выполнять, зарегистрировавшись под ней. Все важные события в системе регистрируются в системном журнале (это называется аудит) вместе с регистрационным именем пользователя, который совершил это событие. То есть эта учетная запись служит для отслеживания, кто из администраторов произвел изменения в сети, когда и какие. Если бы все они работали под одним именем `Administrator`, то по прошествии некоторого времени невозможно было бы выяснить, кто за что отвечает.

А учетную запись `Administrator` следует оставить для крупнейших работ в сети: создания сети, изменения ее общих параметров, разбиения на подсети и т.п. Пароль к этой учетной записи следует охранять особенно тщательно.

Учетную запись для обычной работы мы уже создали ранее — это учетная запись IT1. Теперь создайте учетную запись для административных работ (назовите ее, например, `ITManager1`) и включите ее в группы `Domain Admins` и `Group Policy Creator Owners`.

Если на предприятии несколько администраторов, создайте по паре учетных записей и для них. Не забудьте включить их обычные учетные записи в группы, обеспечивающие доступ к хранилищу документов фирмы (G IT regular и G IT power).

15.2. Инструменты управления сетью

До сих пор мы, сидя за сервером, работали с консолями **Active Directory — пользователи и компьютеры**, **Active Directory — сайты и службы**, консолями управления службами DNS и DHCP, оснастками **Управление компьютером** и **Просмотр событий**. Но в группе **Пуск → Администрирование** на рабочей станции под управлением Windows XP Professional вы видите только **Просмотр событий** и **Управление компьютером** (локальным).

Для того чтобы сделать возможным управление сервером, нам нужно переместить инструменты управления с сервера на рабочую станцию. К счастью, это совсем не сложный процесс.

15.2.1. Установка консоли управления

Установка консоли управления производится следующим образом:

1. Зарегистрируйтесь на рабочей станции под административной учетной записью `ITManager1`.
2. Вставьте в привод инсталляционный компакт-диск с операционной системой Windows Server 2003.
3. Выполните команду **Пуск → Выполнить** и нажмите кнопку **Обзор**. Перейдите в папку `E:\i386` (здесь E: — обозначение компакт-диска) и выберите файл ADMINPAK.MSI. Нажмите **OK**. Будет запущен Мастер установки пакета администрирования системы Windows Server 2003. Нажмите **Далее** и следуйте указаниям Мастера.

Посмотрите, какие утилиты появились в группе **Пуск → Администрирование**. Для проверки выполните следующее:

1. Запустите консоль управления DHCP. Вы увидите пустое окно.
2. В левой части окна щелкните правой кнопкой мыши по значку DHCP и из контекстного меню выберите команду **Добавить сервер**.
3. В диалоговом окне **Добавить сервер** вы увидите сервер `srv001.study.local`. Установите флажок **Авторизованный сервер** и нажмите **OK**. В окне консоли появится сервер DHCP, конфигурация которого соответствует той, что вы произвели, работая непосредственно за сервером.

15.2.2. Совместимость инструментов управления

Для определения того, какой пакет администрирования с какой операционной системой совместим, руководствуйтесь следующими правилами:

- На Windows XP Professional можно установить пакет ADMINPAK.MSI только с установочного компакт-диска системы Windows Server 2003.
- С помощью инструментов системы Windows XP Professional можно управлять серверами Windows Server 2003 и Windows 2000 Server.
- На Windows 2000 Professional можно установить пакет ADMINPAK.MSI только с установочного компакт-диска системы Windows 2000 Server.
- С помощью инструментов системы Windows 2000 Professional можно управлять серверами Windows Server 2003 и Windows 2000 Server.
- На русифицированные версии Windows XP Professional и Windows 2000 Professional можно установить и англоязычный пакет администрирования.

15.3. Работа с инструментами управления

Для начала плохая новость. Не все инструменты, необходимые для управления сетью, устанавливаются из файла ADMINPAK.MSI. Теперь хорошая: если вы немного покопаетесь в системе, вы их найдёте. В меню **Пуск** разработчики компании Microsoft поместили чаще всего используемые инструменты управления.

Многим администраторам действительно в течение всей их работы с системой Windows Server 2003 другие средства для управления сетью не понадобятся. Однако они существуют, и в этой главе мы скажем, как их найти.

Примечание.

Вас не раздражает, что после установки пакета администрирования в главном меню всё время появляется сообщение о том, что появились новые программы? Если да, то откройте окно свойств главного меню, на вкладке **Меню «Пуск»** нажмите кнопку **Настроить**, перейдите на вкладку **Дополнительно** и снимите флажок **Выделять недавно установленные программы**.

Консоль MMC (Microsoft Management Console)

Консоль MMC составляет основу каждой оснастки — инструмента управления системой Windows 2000 и более новых версий. Это легко увидеть:

если вы запустите сразу несколько оснасток, вы убедитесь, что они похожи по внешнему виду, устройству и принципу работы. Времена, когда управление учетными записями пользователей было совсем не похоже на управление службами, давно прошли.

Очень любопытной оснасткой, служащей для управления безопасностью компьютера, является оснастка **Шаблоны безопасности**. Это как раз один из тех инструментов управления, которого нет в главном меню системы Windows XP Professional. Тогда как его запустить?

1. Зарегистрируйтесь на рабочей станции под административной учетной записью. Отныне мы будем понимать под ней только запись ITManager1.
2. Выполните команду **Пуск → Выполнить** и в поле **Открыть** введите `mmc`. Отобразится пустая консоль MMC. Разверните ее окно во весь экран.
3. Выберите команду **Консоль → Добавить или удалить оснастку**. Откроется диалоговое окно с тем же названием, представляющее содержание левого подокна консоли MMC.
4. На вкладке **Изолированная оснастка** нажмите кнопку **Добавить**. В появившемся списке вы найдете как те оснастки, которые уже присутствуют в группе **Администрирование**, так и скрытые. Выберите из списка **Шаблоны безопасности** и нажмите **Добавить**. Закройте все диалоговые окна.

Консоль MMC служит не только для запуска оснасток, которых нет в главном меню. Она позволяет создавать также собственные оснастки для управления сетью.

Допустим, вы ставите себе задачи: следить за работой служб, отслеживать события и наличие места на диске на нескольких компьютерах (мы будем рассматривать один сервер SRVR001 и одну рабочую станцию PC001). Вы можете создать по одной оснастке для каждой задачи, объединив в ней управление несколькими компьютерами, или по одной оснастке для каждого компьютера, объединив в ней несколько задач. Выбор зависит только от вашего стиля управления: время, затрачиваемое на эту работу, в обоих случаях будет одинаково.

Создание собственной оснастки для администрирования одного компьютера

Для создания собственной оснастки для администрирования одного компьютера выполните следующие действия:

1. Зарегистрируйтесь на PC001 под именем `ITManager1`. Запустите пустую консоль MMC.

2. Добавьте в неё оснастку **Службы**. Когда вы будете добавлять модуль, вам нужно будет определить, на данном или на другом компьютере вы хотите этими службами управлять. Установите переключатель в положение **Локальным компьютером** и нажмите **Готово**.
3. Точно так же добавьте оснастки **Просмотр событий** и **Управление дисками**. Закройте окно **Добавить/удалить оснастку** нажатием кнопки **OK**.
4. Выберите из меню **Консоль** команду **Сохранить как** и в поле **Имя файла** введите название новой консоли (например, «Управление PC001»). По умолчанию вам будет предложено сохранить новую оснастку в папке «Администрирование», но в группе **Пуск → Администрирование** вы ее после этого не найдете. Она появится в группе **Пуск → Все программы → Администрирование**. Чтобы не путаться, сохраните новую оснастку просто на рабочем столе.

Проделайте те же шаги, чтобы создать вторую оснастку для управления сервером SRVR001, и сохраните ее на рабочем столе под именем «Управление SRVR001».

Создание собственной оснастки для администрирования одной службы

Для создания собственной оснастки для администрирования одной службы выполните следующие действия:

1. Зарегистрируйтесь на PC001 под именем `ITManager1`. Запустите пустую консоль MMC.
2. Добавьте в неё оснастку **Службы,** поставив переключатель в положение **Локальным компьютером.**
3. Снова добавьте оснастку **Службы,** поставив переключатель в положение **Другим компьютером**, и введите имя сервера SRVR001.
4. Закройте все диалоговые окна и сохраните новую консоль под именем, например, «Службы PC001, SRVR001».

Повторите те же действия для оснасток **Просмотр событий** и **Управление дисками**.

Примечание.

Будьте внимательны, когда будете создавать консоли для управления несколькими компьютерами. Если во время запуска оснастки один из них окажется недоступен (не отвечает на запросы), то потребуется некоторое время для того, чтобы консоль это «осознала» и продолжила работу с другими компьютерами. До этого момента консоль будет выглядеть так, как будто она зависла.

Если вы переносите свое администраторское рабочее место на другую рабочую станцию, вам не нужно создавать консоли заново — достаточно скопировать созданные файлы на новый компьютер. Если они содержат только оснастки, являющиеся стандартными компонентами системы Windows XP Professional, то эти консоли будут работать сразу же. Если же в них входят инструменты управления сервером, то вам понадобится установить на новой рабочей станции пакет администрирования ADMINPAK.MSI.

Удалённое управление компьютерами с помощью стандартных консолей MMC очень удобно для локальных сетей или для сетей WAN. Консоль использует для подключения к удалённому компьютеру удалённый вызов процедур (Remote Procedure Calls, RPC) и связывается с компьютером, управление которым она проводит, через инструмент WMI (Windows Management Instrumentation).

15.4. Запуск приложений от имени другого пользователя

Вы уже запомнили, что для обычной работы администратор должен регистрироваться под учетной записью с правами рядового пользователя. Допустим, вы вошли под ней, запустили почтовый клиент, Word и Excel, открыли несколько веб-страниц, вступили в беседу по ICQ... и тут звонит пользователь и говорит, что забыл свой пароль. Допустим также, что вы почему-либо не хотите заставлять его ждать. Так что же, закрывать все приложения, завершать сеанс, регистрироваться с правами администратора и назначать ему новый пароль?

В системе Windows XP Professional существует для подобных случаев очень элегантное решение. Вам не нужно ни завершать работу, ни сохранять её, ни уж тем более выходить из компьютера. Достаточно сделать следующее:

1. Откройте группу **Пуск → Администрирование** и щелкните правой кнопкой мыши по консоли **Active Directory — пользователи и компьютеры**.
2. Из контекстного меню выберите команду **Запуск от имени**. Отобразится диалоговое окно **Запуск от имени другого пользователя**, где вы можете указать учетную запись, с правами которой собираетесь запустить эту консоль.
3. Поставьте переключатель в положение **Учетную запись указанного пользователя**, в поле **Имя пользователя** введите `STUDY\ITManager1`, в поле **Пароль** введите свой пароль и нажмите **OK**.

4. Консоль **Active Directory — Пользователи и компьютеры** запустится с правами администратора, и вы сможете сменить пароль своему пользователю. Закройте консоль и продолжите свой сеанс работы под именем рядового пользователя.

Существуют всего два приложения, которые нельзя запустить от имени другого пользователя: это Проводник Windows и Internet Explorer.

15.5. Удалённый рабочий стол

Допустим, вы пришли к пользователю, чтобы разобраться с неполадками на его рабочем месте. По какой-то непонятной причине этот пользователь всё ещё работает в ОС Windows NT 4.0 Workstation. Вам требуется срочно войти с его компьютера на сервер (чтобы удостовериться, например, работает ли та или иная служба, с которой этот пользователь никак не может связаться). Но инструменты управления системы Windows NT 4.0 не работают в домене Active Directory. Что же делать?

Решение существует, но сначала его надо подготовить. В системе Windows Server 2000 оно называется Удалённый рабочий стол, в системе Windows 2000 — Служба Terminal Services.

15.5.1. Как работает Удалённый рабочий стол

Функционирование удаленного рабочего стола основано на том, что от клиента к серверу и обратно передается минимум информации. Клиент посылает только те порции данных, которые получены от внешних устройств (нажатие на клавишу клавиатуры, перемещение мыши, штрихкод, считанный сканером и т.п.). С сервера на клиентский компьютер передается только графический образ экрана, и то не весь, а только та его часть, которая изменяется в данный момент (то есть если вы перемещаете указатель мыши в правом верхнем углу экрана, то изображение левого нижнего угла по сети не передается).

Объём передаваемых данных настолько мал, что при сравнительно низкой скорости соединения (достаточно 14,4 кбит/с) у пользователя (в данном случае администратора) создается впечатление, что он работает прямо за сервером.

Удалённый рабочий стол — это компонент ОС Windows Server 2003, устанавливаемый по умолчанию, но сразу после установки он отключен. Нужно включить эту функцию и указать, каким пользователям разрешен доступ к ней.

1. Зарегистрируйтесь на SRVR001 как администратор. Откройте окно **Свойства системы**.
2. Перейдите на вкладку **Удаленное использование** и установите флажок ***Разрешить удаленный доступ к этому компьютеру***.
3. По умолчанию доступ к удаленному рабочему столу разрешен только членам группы администраторов. Если вы хотите разрешить доступ еще некоторым пользователям (например, своей обычной учетной записи), нажмите кнопку **Выбрать удалённых пользователей** и добавьте их.

15.5.2. Сколько человек могут одновременно работать «за» сервером?

Количество одновременных сеансов работы с удалённым рабочим столом ограничено.

1. Зарегистрируйтесь на SRVR001 как администратор. Запустите консоль **Настройка терминальной службы**.
2. В правой части окна щелкните правой кнопкой мыши по значку **RDP-Tcp** (RDP — это протокол Remote Desktop Protocol) и из контекстного меню выберите команду **Свойства.**
3. Перейдите на вкладку **Сетевой адаптер** и в поле **Максимальное количество присоединений** попытайтесь изменить количество 2 на большее. Это будет невозможно.

   Таким образом, одновременно для рабочего стола может быть открыто не более двух соединений (оба может использовать один и тот же пользователь). Служба Terminal Services в системе Windows 2000 Server в режиме администрирования подчиняется точно такому же ограничению, но в ОС Windows Server 2003 существует дополнительное удобство: третий пользователь может подключиться с рабочему столу, зарегистрировавшись непосредственно на сервере (если у него есть такое право).

   Если вы выполняете за сервером какую-то работу и хотите продолжить её с другого компьютера, то можете подключиться к открытому на сервере сеансу, запустив клиент рабочего стола с аргументом `/console`.
4. Перейдите на вкладку **Разрешения** и проверьте настройку разрешений на доступ к удалённому рабочему столу сервера.

Кажется, что по сравнению с Windows 2000 Server система Windows Server 2003 предлагает дополнительную возможность — подключение к удалённому рабочему столу и тех пользователей, которые не являются членами группы администраторов. По крайней мере, компания Microsoft представляет это так. Но если вы всё же познакомились раньше с воз-

можностями службы Terminal Services системы Windows 2000 Server, то вы могли заметить, что и там существует та же вкладка **Разрешения**, на которой можно добавить в список субъектов доступа рядовых пользователей.

15.5.3. Как подключиться к удалённому рабочему столу

К удалённому рабочему столу можно присоединиться только с помощью специального клиента. Раньше он назывался **Клиент службы Terminal Services**. Теперь существует новая его версия, являющаяся компонентом клиентской ОС Windows XP Professional (и, конечно, серверной Windows Server 2003), которая называется **Подключение к удалённому рабочему столу**.

1. Зарегистрируйтесь на PC001 как администратор.
2. Откройте меню **Пуск → Все программы → Стандартные → Связь** и выберите команду **Подключение к удалённому рабочему столу**.
3. В поле **Компьютер** введите имя или IP-адрес сервера, к которому вы хотите подключиться.
4. Нажмите кнопку **Параметры**. На вкладке **Экран** вы можете отрегулировать величину окна, в котором будет отображаться рабочий стол удалённого компьютера. По умолчанию применяются настройки компьютера, за которым вы работаете.
5. На вкладке **Локальные ресурсы** определяется, какие из средств локального компьютера можно будет использовать при подключении к удалённому компьютеру. Изначально включены только принтеры, но вы можете также добавить диски и последовательные порты. Диски стоит прибавить в том случае, если вы захотите, например, сохранить документ, находящийся в работе на удалённом компьютере, на диск локального компьютера, на котором вы в данный момент работаете. Последовательные порты понадобятся вам, чтобы перенести на сервер данные с устройства для считывания штрих-кодов.
6. На вкладке **Дополнительно** можно выбрать скорость соединения. В зависимости от неё будут или не будут доступны остальные стандартные функции системы (например, отображение содержимого окна при его перетаскивании).
7. Настройки подключения можно сохранить, нажав кнопку **Сохранить как** на вкладке **Общие**.
8. Нажмите кнопку **Подключить**. Отобразится стандартное окно входа в систему, в котором вы должны ввести имя и пароль пользователя, у которого есть право на подключение. После этого вы можете работать с сервером так, как если бы вы сидели прямо за ним.

Для клиентских операционных систем версий, предшествующих Windows 2000, где нельзя установить новый пакет администрирования, возможность подключаться к удалённому рабочему столу является существенным подспорьем. Но клиент подключения еще нужно установить.

Если клиентский компьютер работает под управлением Windows версии более новой, чем 9x и ME, то можно установить клиент с установочного компакт-диска Windows XP Professional или Windows Server 2003. Вставьте компакт-диск в привод, дождитесь автозапуска и выберите задачу **Другие задачи → Установить подключение к удалённому рабочему столу**. Далее поступайте согласно указаниям Мастера установки.

Вы можете устанавливать клиент также по сети, из общей папки, содержащей его инсталляционные файлы:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Запустите Проводник и перейдите в папку `%SYSTEMROOT%\system32\clients`. Вас интересует подпапка `tsclient`. Откройте к ней сетевой доступ и настройте разрешения так, чтобы предоставить пользователям только разрешение «Чтение и запуск».
3. Для установки клиента подключения запустите из этой папки файл `win32\setup.exe` с правами администратора.

Если у вас установлена старая версия клиента для подключения к удалённому рабочему столу, вы можете использовать и её тоже. Новый клиент системы Windows XP Professional можно использовать для доступа к службе Terminal services системы Windows 2000 Server.

Клиент для подключения к удалённому рабочему столу есть даже в ОС Windows PocketPC 2002, работающей на карманных компьютерах. То есть даже с такого компьютера вы можете управлять своим сервером! Это, конечно, не так удобно, но в случае необходимости вполне возможно.

Огромной выгодой функции Удалённый рабочий стол является возможность доступа к ней через Интернет. Для этого необходимо открыть единственный порт — 3389 протокола TCP и запросы, адресованные на этот порт, переадресовать на соответствующий сервер внутри сети. Различные типы коммуникации между клиентом для подключения к удалённому рабочему столу и самим сервером шифруются автоматически (включая саму регистрацию), то есть, таким образом, возможность перехвата и нанесения вреда передаваемым данным минимальна.

15.5.4. Удалённый рабочий стол в Windows XP Professional

Windows XP Professional — это первая клиентская операционная система, к которой можно подключиться удаленно благодаря тому, что она располагает функцией Удалённый рабочий стол. В Windows 2000 Professional этой функции еще не было.

Это значит, вы можете не ходить проверять жалобы пользователя на его рабочее место, а работать за его компьютером, не вставая со своего стула.

К сожалению, функциональность удаленного рабочего стола в клиентской операционной системе довольно ограничена. Одновременно для рабочего стола может быть открыт только один сеанс, то есть, если к рабочему столу пользователя подключитесь еще и вы, то локальный пользователь будет отключен, а его работа не сохранится. В таблице 15.1 показано, что происходит, когда к рабочему столу компьютера, за которым работает пользователь `Shop1`, подключаются другие.

Последствия подключения к удаленному рабочему столу Windows XP Professional *Таблица 15.1*

Кто подключается	Последствия	Комментарии
Shop1 с другой рабочей станции	Сеанс локального пользователя будет заблокирован. После окончания сеанса удалённой работы его можно возобновить	Удаленный пользователь Shop1 подключается к открытому локальному сеансу и может продолжать работу с того места, на котором прервал ее, отходя от компьютера (то же самое происходит при запуске Клиента подключения к удалённому рабочему столу с аргументом /console)
Локальный администратор	Сеанс локального пользователя будет остановлен, а после окончания работы администратором сеанс будет закрыт	Локальный пользователь Shop1 лишится всех своих несохранённых документов и впоследствии не сможет сам открыть новый сеанс работы (это сможет сделать только локальный администратор)

15.5.5. Комбинации клавиш в сеансе удалённого рабочего стола

Когда вы подключаетесь к рабочему столу сервера, в верхней части экрана появляется панель с именем или IP-адресом удалённого компьютера (в зависимости от того, что вы задали в окне параметров подключения). В предыдущих версиях клиента подключения к службе Terminal Services этой панели не было.

Назначение трёх кнопок управления в правом углу панели понятно — речь идёт о работе с окном (свернуть, развернуть и закрыть). Значок булавки в левом углу позволяет закрепить панель на рабочем столе или

автоматически скрывать ее, как только вы отведете от нее указатель мыши.

Работая за удаленным столом, вы не можете пользоваться стандартными комбинациями клавиш Windows, потому что они перехватываются и обрабатываются локально. Если вы хотите, чтобы нажатие комбинации клавиш обрабатывалось на удаленном компьютере, нажимайте вместо нее эквивалентную комбинацию (табл. 15.2).

Эквиваленты стандартных комбинаций клавиш в сеансе удалённого рабочего стола *Таблица 15.2*

Стандартная комбинация	Эквивалент	Назначение
	Ctrl+Alt+Break	Свертка/восстановление окна удалённого рабочего стола
Ctrl+Alt+Del	Ctrl+Alt+End	Вызов диспетчера задач системы Windows
Alt+Tab	Alt+Page Up	Переключение между окнами приложений
Alt+Shift+Tab	Alt+Page Down	Переключение между окнами приложений в обратном направлении
Alt+Esc	Alt+Insert	Переключение между окнами приложений в порядке их запуска
Print Screen	Ctrl+Alt+минус (на цифровой клавиатуре)	Копирование в буфер обмена изображения рабочего стола
Alt+Print Screen	Ctrl+Alt+плюс (на цифровой клавиатуре)	Копирование в буфер обмена изображения активного окна

15.5.6. Отключение и завершение сеанса

Если вам нужно закончить сеанс удалённого рабочего стола и у вас отображена панель, решение выглядит весьма простым — щелчок по крестику, как для обычного окна приложения. Однако таким образом вы не завершите сеанс, а отключитесь.

Отключение

Когда вы отключаетесь от удалённого рабочего стола, происходит следующее:

- Связь между локальным компьютером и рабочим столом сервера прерывается.
- Сеанс удалённого рабочего стола на сервере остается открытым, так что впоследствии вы снова сможете подключиться к нему и продолжить работу с того же самого места.

Отключение можно рекомендовать в среде, где для рядовых пользователей открыт доступ к Терминальной службе, чтобы они могли запускать на сервере задания, занимающие много времени, а через несколько часов подключаться снова и смотреть на результаты расчета.

В нашем случае, когда максимальное количество сеансов ограничено двумя (плюс один локальный), отключение сеанса представляет проблему. Достаточно двух отключений, и к удалённому рабочему столу уже больше никто не подключится, так что постарайтесь подобной ситуации избегать.

Завершение сеанса

Когда вы завершаете сеанс удалённого рабочего стола, происходит следующее:

- Связь между локальным компьютером и рабочим столом сервера прерывается.
- Сеанс удалённого рабочего стола на сервере закрывается, и другой пользователь сможет начать новый сеанс.

Чтобы завершить сеанс, выполните команду **Пуск → Завершить работу** из главного меню, которое вы видите на рабочем столе сервера. Только будьте осторожны в диалоговом окне **Завершение работы Windows:** если вместо **Завершение сеанса** вы выберете **Выключение**, то удалённый компьютер и вправду выключится. Нелишним будет снова напомнить, что назначением функции Удалённый рабочий стол является создание у пользователя впечатления, что он сидит непосредственно за сервером.

15.6. Итоги

Никогда не работайте под учётной записью с правами администратора, если можете этого избежать: тогда при атаке вирусов или других неприятностях повреждения системы будут минимальны. Для текущего управления сетью заведите каждому из администраторов отдельную учетную запись, по которой вы сможете отличать в системном журнале, кто внес в сеть какое изменение. Включите эти учетные записи в группу администраторов домена.

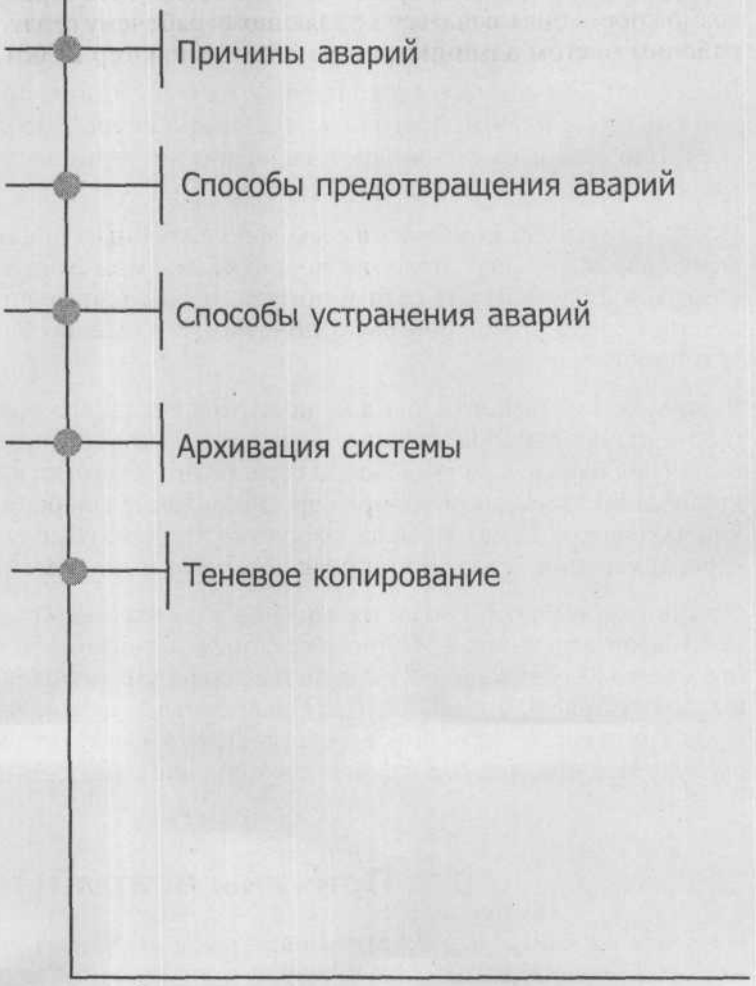
Если вы не хотите постоянно сидеть в серверной, чтобы управлять сетью, то вам следует установить пакет администрирования на ту рабочую станцию, которая станет вашим рабочим местом. Так в вашем распоряжении будут те же инструменты управления, что и на сервере. Пакет администрирования устанавливается из файла ADMINPAK.MSI, который находится на установочном компакт-диске с серверной операционной системой.

Другая возможность управления сервером с рабочей станции — это использование Удалённого рабочего стола. На рабочей станции должен быть установлен клиент подключения к удалённому рабочему столу. Эту возможность можно использовать с рабочих станций, где стоит старая операционная система, на которую нельзя поставить пакет администрирования.

Состояние сети

Мы установили на рабочую станцию PC001 пакет утилит для управления сервером SRVR001 и доменом Active Directory. На сервере мы включили возможность подключаться к удаленному рабочему столу. Таким образом, рабочим местом администратора стал компьютер PC001.

Глава 16 Что если сервер рухнет завтра?



Если завтра, то ничего страшного. У нас ещё много времени, чтоб хорошенько к этому подготовиться. Однако сервер может совершенно спокойно выйти из строя через час, через четверть часа или даже через минуту. Готовы ли мы к этому? Нет!

Поскольку в этой книге мы имеем дело с учебным предприятием, которому авария сервера никак не повредит, мы можем прежде всего ознакомиться с элементами сети и домена, чтобы впоследствии при произнесении слова архивация было понятно, что именно будет необходимо архивировать.

В реальной обстановке, однако, подготовка к такого рода неполадкам в сети является одной из главных задач администрирования и производится ещё перед началом работы любой сети. Более того, если в сети проводятся какие-либо изменения (например, обновление операционной системы контроллера домена), необходимо чётко продумать не только план и методы архивации сети, но и определить стратегию внесения изменений.

Обычно речь идёт об области, которая в случае недооценки может привести в организации к неприятным последствиям. Наоборот, в случае правильно продуманной стратегии и выполнения определённых действий вы можете спать спокойно. Быть уверенными в том, что проблемы не возникнут, на сто процентов нельзя. Но тот факт, что в любой момент вы будете знать, что делать, является большим плюсом.

16.1. Причины аварий

Не стоит ожидать, что из этого параграфа вы узнаете о чем-то новом для себя. Задача подготовки к аварии и ликвидации ее последствий настолько тривиальна, что не требует от администратора почти никаких способностей. Кроме одной — ни о чём не забывать.

Ошибки программного обеспечения

Ошибки программного обеспечения существуют всегда. Ответственность за исправление некоторых из них (например, в ядре операционной системы) лежит полностью на производителе. Ущерб от других может уменьшить и администратор: например, обнаружив ошибку в драйвере, приводящую к нарушению работы устройства, найти и установить более свежую его версию.

Сбои оборудования

Компоненты компьютера — это технически сложная аппаратура, и даже гарантия производителя не может служить ручательством, что в один прекрасный день устройство не «вздохнёт в последний раз». Сломаться в компьютере может все что угодно. Очевидно, что крах жёсткого диска сервера потребует намного больше работы, чем неполадки с мышью.

Ошибки пользователей

Рядовой пользователь не имеет в системе Windows XP Professional таких прав и полномочий, чтобы быть способным своей оплошностью нанести ощутимый вред функциям отдельного компьютера или даже всей сети. Нужно сказать, что защита от возможных ошибок пользователей рассматривалась уже при создании операционных систем, основанных на технологии NT, так что у пользователей нет полномочий, ненужных для их работы. Ошибок пользователей избежать нельзя, поэтому рекомендую заняться их предотвращением. Не стоит надеяться на то, что пользователь будет способен чему-то научиться или что-то понять. Лучшим подходом будет подобрать для него из многих решений самое простое.

Ошибки администраторов

Одной из причин ошибок администраторов является недостаток знаний. Вследствие того, что администраторам предоставляется в системах полная свобода, их ошибки могут нанести системе вред. Понятно, что чем больше у администратора прав, тем больше неприятностей он сможет причинить своими непрофессиональными действиями.

Умышленный вред

Здесь бессмысленно разбираться, чья это была ошибка — пользователя или администратора. Результат, в любом случае, всегда отрицательный и требует неимоверных усилий для возвращения в первоначальное или, по крайней мере, стабильное состояние.

Непреодолимая сила

Примерно в пяти процентах случаев выхода системы из строя никто не может сказать, что было тому причиной. Бывает, что простая перестановка кабелей питания возвращает технику к жизни. Против Высшей Силы нельзя найти стопроцентно эффективное решение. Всегда, хотя речь идёт об очень маловероятной возможности, нужно приготовиться к самому худшему, и скорее всего без шаманства будет не обойтись.

16.2. Способы предотвращения аварий

То, что проблемы рано или поздно возникнут, понятно всем. Далее следует вопрос, настанет ли всеобщий хаос или же проблемы будут решаться с помощью продуманных действий, систематически, без лишних эмоций и эффективно. Думаю, мы сойдёмся на том, что гораздо лучше, чем необдуманно решать проблемы, будет посвятить время их предотвращению.

Поскольку у нас в сети стоит операционная система Microsoft Windows, давайте познакомимся с вариантами решения проблем, которые корпорация Microsoft нам предоставляет вместе со своей продукцией.

16.2.1. Ошибки программного обеспечения

Драйверы

Возможно, что на практике вы сталкивались со следующей ситуацией. На своём компьютере вы обновили драйвер графической карты. На сайте изготовителя обещаны прирост скорости, частоты развертки и поддержка новой версии DirectX.

После установки вы, однако, обнаруживаете, что что-то здесь не так. Не только графическая карта не показывает никаких признаков улучшения, но у вас также возникают проблемы с другими компонентами, и более того — вам кажется, что операционная система больше не работает так же быстро и хорошо, как до установки нового драйвера.

Где же проблема? Скорее всего, в новом файле. И всё равно, повесил ли производитель на своём сайте ещё недоделанную версию, которую по ошибке назвал пригодной для поставки, или программное обеспечение не прошло необходимого тестирования. Вас интересует, как можно удалить новую версию драйвера и вернуть старую.

Возможно ли, чтобы из-за некорректной версии драйвера замедлилась работа всей операционной системы? Да, поскольку в драйвер устройства

могут входить не только файлы управления устройством, но и системные библиотеки. Они послужат источником неприятностей с любыми устройствами, драйвера которых используют эти библиотеки.

Избежать этого в системе Windows XP Professional не так уж и сложно. Первый шаг — это установка только проверенных драйверов оборудования. Цифровая подпись компании Microsoft в драйвере устройства означает, что данное оборудование было протестировано с дополнительным программным обеспечением и что оно не вызывает в системе Windows XP Professional никаких неполадок.

Другой вариант — резервное копирование всей системы перед установкой драйвера неизвестного происхождения. Это, однако, экстремальный случай, как мы увидим в следующей части главы, где будем рассматривать способы устранения неполадок.

Операционные системы и приложения

Ошибки операционных систем и приложений может исправить исключительно их производитель — компания Microsoft и другие. Как пользователи мы можем с ними встретиться в форме пакетов исправления или обновления (hotfix, QFE, Service Pack).

Силами администратора ошибки операционных систем предотвратить нельзя. Но можно настроить автоматическую установку исправлений на все компьютеры в сети. Это поможет поддерживать сеть в стабильном состоянии.

16.2.2. Сбои оборудования

Поскольку компьютер можно представить как совокупность отдельных устройств, проблемы технического характера напрямую связаны с тем, что случится, если сломается то или иное устройство. Надо предвидеть эту ситуацию и задумываться над тем, как ее

Если не иметь в виду те случаи, когда у нас уже припасён ещё один сервер, идентичный текущему и не трогать область кластеров (которые, по понятным причинам, также не являются стопроцентным решением), мы можем разделить поломки оборудования на две группы.

Выход из строя жесткого диска или утрата данных

Речь идёт о классическом случае, когда жёсткий диск ломается физически (ломается механическая или электронная часть). Решением проблемы является создание массива RAID (Redundant Array of Independent Disks, избыточный массив независимых дисков).

Существуют пять основных уровней RAID. Уровень 0 (чередующийся массив) представляет собой несколько дисков, данные на которые записываются порциями поочередно. Он дает выигрыш только в скорости чтения/записи, но не в надежности хранения данных. Уровень 1 (зеркальный массив) — это два или более дисков, данные на которых дублируются. Этот уровень обеспечивает не только ускорение чтения данных, но и позволяет восстановить их в случае выхода из строя одного из дисков. Платой за надежность является неэффективное расходование дискового пространства.

Чаще всего встречается уровень RAID-5 (чередование с контрольной суммой), при котором данные поочередно записываются большими блоками на все диски массива, а контрольные суммы хранятся на всех дисках. Массив RAID-5 можно создать, если у вас есть не менее трех дисков, при этом использоваться будет 66% их емкости. Другие уровни RAID можно рассматривать как комбинацию 0, 1 и 5.

В нашей сети о подобных возможностях мы можем только мечтать, поскольку жесткий диск у нас даже на сервере только один. На рабочих станциях под управлением Windows XP Professional дисковые массивы RAID создать вообще нельзя. Здесь необходимо найти другой способ предотвращения потерь. Проще всего будет сделать так, чтобы на рабочих станциях не хранились никакие важные данные. Подробнее об этом будет сказано в главе 17.

Выход из строя других устройств

Сюда относятся, например, поломка источника питания, сетевой карты и т.д. Решение этих проблем во многом зависит от финансовых возможностей предприятия. Одной крайностью является уже упомянутое хранение запасного сервера вне сети.

На рабочих станциях проблемы поломки решаются таким образом, что у организации есть в запасе один или несколько полностью оснащённых компьютеров, которые и предоставляются пользователям взамен вышедших из строя. Или же некоторое количество запасных частей, которые устанавливаются вместо испорченных.

Проблемы с электропитанием

К сбоям оборудования относятся и отключение или перепады напряжения в электросети, последствия которых могут быть катастрофическими. Решением является приобретение источников бесперебойного питания (UPS). Если финансовые возможности предприятия не позволяют защитить от проблем с питанием все компьютеры, то нужно обеспечить бесперебойным питанием хотя бы серверы, принтеры и важнейшие из рабочих станций.

Ошибки

Ошибки может совершить каждый. Чтобы предотвратить большинство ошибок пользователей, просто запретите им делать то, чего им делать не полагается, и обучите тому, что знать просто необходимо.

Предотвратить ошибки администраторов гораздо труднее. Поскольку администратор — это по определению тот, чьи полномочия ограничить нельзя, он имеет все права, даже такие, о которых сам толком не знает, и властен причинить сети огромный ущерб. Чтобы администраторы не допускали ошибок, им надо постоянно учиться.

Умышленный вред

К тому, что будет сказано в главе 22, посвященной безопасности сервера и сети, можно добавить только необходимость затруднения физического доступа злоумышленника к уязвимым местам сети: железная дверь и прочный замок на серверной, запирание рабочих мест пользователей по окончании рабочего дня и т.п.

Непреодолимая сила

Регулярное резервное копирование.

16.3. Способы устранения аварий

Совершенно точно мы можем сказать, что важнейшим компьютером в сети является сервер (или сервера). Возникает вопрос, имеет ли вообще смысл беспокоиться о компьютерах пользователей. Если вы как администратор обеспечите пользователям возможность хранить документы только на сервере, вопрос о восстановлении данных будет решаться просто.

Здесь мы детально рассмотрим почти все средства, которые есть в нашем распоряжении для устранения неполадок.

16.3.1. Драйверы

Цифровая подпись драйвера

Первым шагом в обеспечении стабильности системы является установка только подписанных драйверов (проверенных и совместимых с системой). Действия системы при попытке установки неподписанного драйвера можно посмотреть на вкладке **Оборудование** в диалоговом окне **Свойства**

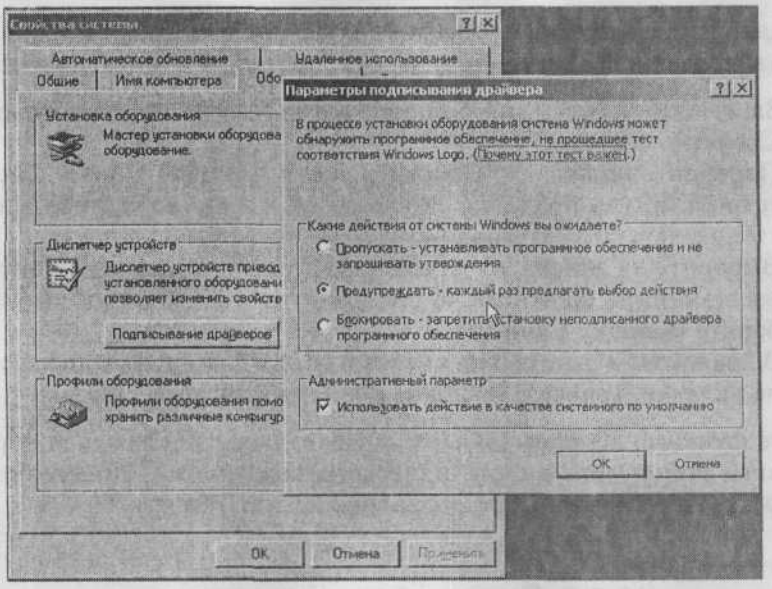


Рис. 16.1. *Диалог выбора реакции системы на установку неподписанного драйвера.*

системы. По умолчанию стоит режим предупреждения с возможностью выбора дальнейшего действия.

В исходной конфигурации при попытке установить драйвер без цифровой подписи компании Microsoft появится предупреждение с вопросом, действительно ли вы хотите установить данный драйвер. Если выбран первый пункт, никакого контроля подписей происходить не будет и драйвер будет установлен без вопросов. Если же выбран третий пункт, неподписанный драйвер установлен не будет.

Поскольку устанавливать оборудование могут только те, кто обладает правами локального администратора, у рядовых пользователей этот переключатель деактивирован.

Откат к предыдущей версии

Система Windows XP Professional как продукт компании Microsoft предоставляет возможность автоматического возврата предыдущего драйвера оборудования, если вы недовольны его обновлением. Каждый, кто пытался вручную откатить драйвер в предыдущих версиях Windows, оценит это нововведение.

Когда вы обновляете некоторый драйвер, в папке `%SYSTEMROOT%\system32` создается подпапка с названием `ReinstallBackups`, в которую

помещается предыдущая версия этого драйвера. Чтобы впоследствии вернуться к последней сохраненной версии, поступите следующим образом:

1. Зарегистрируйтесь как администратор. Откройте диалоговое окно **Свойства системы**.
2. Перейдите на вкладку **Оборудование** и нажмите кнопку **Диспетчер устройств**. Отобразится список оборудования, установленного в компьютере, по категориям.
3. Выберите из списка то устройство, драйвер которого вы хотели бы восстановить, щелкните по его значку правой кнопкой мыши и выберите команду **Свойства**.
4. В диалоговом окне свойств оборудования нажмите кнопку **Откатить** на вкладке **Драйвер**. Всё остальное предоставьте системе.

Эти две функции исчерпывающим образом показали вам, как устранять неполадки с оборудованием технического обеспечения. Ничего большего с устройствами Plug-and-Play проводить не требуется.

16.3.2. Система не загружается

Эта проблема возникает именно тогда, когда никто не ожидает подвоха, и обычно производит на пользователя самый ошеломляющий эффект. Чаще всего ее причиной бывает изменение аппаратной или программной конфигурации компьютера, выполненное перед его последним выключением. Это может быть обновление драйвера, установка приложения или изменение состояния службы (включение режима автозапуска). Можно попробовать запустить систему в той конфигурации, которая была еще работоспособна.

Последняя удачная конфигурация

Чтобы загрузить систему в режиме последней удачной конфигурации, нажмите в процессе загрузки клавишу F8 и выберите из появившегося меню соответствующую команду.

В результате та ветвь реестра, где хранятся сведения о последней удачной конфигурации, будет прочитана вместо ветви HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet, хранящей сведения о текущей конфигурации, и таким образом настройки, сделанные непосредственно до аварии, не сработают.

Этот режим не поможет, когда компьютер зависает сразу после регистрации пользователя. Дело в том, что последней удачной конфигурацией считается та, в которой операционная система смогла загрузиться и выполнить регистрацию пользователя. Эта (текущая) конфигурация и записывается в реестр в качестве удачной.

Безопасный режим

Если не удаётся запустить компьютер в режиме последней удачной конфигурации, вы можете попробовать Безопасный режим. В этом режиме запускаются только те службы и загружаются только те драйвера, без которых невозможно обойтись: так, звуковая карта и порт USB работать не будут, а новейшая видеокарта будет работать под управлением стандартного драйвера, использующего лишь малую часть ее возможностей. Полученная таким образом рабочая среда пригодна не для повседневной работы, а для диагностики и ремонта.

Загрузка в безопасном режиме — единственный вариант загрузки, при котором не обновляются сведения о последней удачной конфигурации.

Оба вышеназванных режима могут помочь в случаях, когда загрузка не происходит по вине изменения конфигурации системы. Если система не загружается из-за повреждения или отсутствия важного файла (например, загрузчика NTLDR), то конфигурация здесь ни при чем и для восстановления нужно использовать другие инструменты.

Консоль восстановления

Этот инструмент не предлагает графического интерфейса — только интерфейс командной строки, в которой можно вводить команды для копирования файлов, ремонта загрузочных областей жесткого диска (**fixmbr**, **fixboot**) и работы с разделами диска (**diskpart**, **format**), включения и выключения автозапуска служб (**enable**, **disable**). Список всех доступных команд можно вывести по команде **help**, а чтобы получить справку по назначению и использованию конкретной команды, введите эту команду с ключом **/?**.

Огромным плюсом Консоли восстановления является возможность работать с разделами, отформатированными файловой системой NTFS.

Другое преимущество Консоли восстановления состоит в том, что она находится на установочном компакт-диске Windows XP Professional. Операционную систему предыдущей версии (Windows NT 4.0) при повреждении системных файлов можно было загрузить и ремонтировать только со спасательной дискеты, которую мало кто считал нужным создавать.

Сейчас мы намеренно повредим системные файлы на компьютере PC001, а потом исправим разрушения с помощью Консоли восстановления.

Примечание.

Хотя предлагаемые вам действия вполне безопасны, важные файлы с PC001 лучше все-таки предварительно сохранить в другом месте.

1. Приготовьте установочный компакт-диск Windows XP Professional.
2. Зарегистрируйтесь на PC001 как администратор.
3. Удалите файл **C:\NTLDR**. Если вы его не видите, включите режим отображения скрытых и системных файлов.
4. Перезагрузите компьютер. Операционная система не запустится, вместо этого появится сообщение о том, что NTLDR не найден.

Для восстановления системы выполните следующие действия:

1. Смените в BIOS компьютера PC001 порядок загрузки так, чтобы первым просматривался компакт-диск.
2. Вставьте в CD-привод установочный компакт-диск Windows XP Professional и перезагрузите компьютер.
3. Нажмите любую клавишу. Начнется первая стадия загрузки, совпадающая с началом установки операционной системы.
4. Дождавшись появления текстового окна **Windows XP Professional Setup (Установка Windows XP Professional)**, нажмите клавишу Enter.
5. В окне **Setup Welcome (Вас приветствует программа установки)** нажмите клавишу R — запуск Консоли восстановления.
6. Вы увидите список установленных на данном компьютере операционных систем, из которых вам предлагается выбрать подлежащую восстановлению, введя ее номер. У вас установлена всего одна система, поэтому введите 1 и нажмите клавишу Enter.
7. Теперь необходимо ввести пароль локального администратора, назначенный во второй главе при установке операционной системы на данный компьютер. До сих пор вы обходились полномочиями доменного администратора и только сейчас видите, зачем нужен пароль администратора локального и как важно его надежно хранить. Если вы переименовали учетную запись локального администратора, введите пароль этой переименованной записи.
8. Запасной файл загрузчика находится на компакт-диске. Скопируйте его в корень диска C:

```
copy e:\i386\ntldr c:\
```

   (здесь E: — это обозначение компакт-диска).
9. Для перезагрузки компьютера извлеките компакт-диск из привода и введите команду **exit**.

Итак, с помощью Консоли восстановления мы в течение нескольких минут решили довольно сложную проблему. Но в конфигурации по умолчанию функциональность Консоли восстановления несколько ограничена:

- Нет возможности получить доступ к папкам `Program Files`, `Documents and Settings`.
- Нельзя копировать файлы с жёсткого диска на дискету.

Чтобы снять эти ограничения, предпримите следующие шаги:

1. Зарегистрируйтесь на PC001 как администратор. Если вы уже зарегистрированы как рядовой пользователь, выполняйте дальнейшие действия от имени администратора.
2. Запустите консоль **Active Directory — пользователи и компьютеры**. Откройте окно свойств домена `study.local`.
3. Перейдите на вкладку **Групповая политика** и раскройте объект Default Domain Policy.
4. Разверните ветвь **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности**.
5. В правой части окна консоли выберите политику **Консоль восстановления: Сделать возможным копирование дискет и доступ ко всем файлам и папкам(Recovery console: allow floppy copy and access to all drives and all folders)** и установите флажки **Определить указанный ниже параметр политики** и **Включить.** Закройте все окна.

Настроив таким образом локальную политику безопасности на всех компьютерах домена, вы сможете во время работы с Консолью восстановления иметь доступ ко всем папкам и копировать файлы в обоих направлениях.

В рассмотренном случае, когда система не загружалась из-за повреждения загрузчика, запуск Консоли восстановления с установочного компакт-диска был единственным выходом. Но чаще все-таки бывает, что Консоль восстановления нужна для того, чтобы отключить автоматический запуск той службы, из-за которой возникли проблемы с загрузкой. На такой случай удобнее установить ее в качестве альтернативной операционной системы.

Чтобы установить Консоль восстановления на сервер:

1. Зарегистрируйтесь на SRVR001 как администратор. Вставьте в привод установочный компакт-диск Windows Server 2003.
2. Выполните команду **Пуск → Выполнить** и в поле **Открыть** введите команду

```
D:\i386\winnt32.exe /cmdcons
```

   (здесь E: — это обозначение компакт-диска).
3. В диалоговом окне с информацией об установке Консоли восстановления ответьте **Да**. Установка произойдёт автоматически.

Рекомендуется всегда устанавливать Консоль восстановления сразу же после установки операционной системы, хотя бы на серверы. Это позволит сэкономить время в случае неполадок.

16.4. Архивация системы

В операционной системе Windows 2000 с архивацией произошли значительные изменения в лучшую сторону. Архивация стала доступнее и появилась возможность проводить её на локальный диск или на удалённый компьютер.

Архивация системы — это не просто сохранение важных документов. Существенной частью этого процесса является сохранение настроек и параметров системы — то есть состояние реестра, пользовательских учётных записей и т.п. В Windows NT 4.0 архивация состояния системы была постоянной головной болью администраторов, которым каждый раз приходилось решать, что именно подлежит сохранению — весь реестр или некоторая его часть, файл с учетными записями или что-то ещё. Все эти неясности прояснила программа архивации, появившаяся в Windows 2000 и унаследованная системой Windows XP Professional. В серверных операционных системах, начиная с Windows 2000 Server, средства архивации были дополнительно усовершенствованы.

Что сохранять

Каждый администратор хорошо знает, что целью архивации является последующее успешное восстановление данных. Под понятием успешного восстановления, однако, каждый подразумевает что-то свое. Если для пользователя успешным считается восстановление доступа к его файлам, хранящимся на сервере, то для администратора успех — это полное восстановление всего сервера (запуск сетевых служб, функционирование приложений или базы данных, авторизация пользователей на контроллере домена и т.п.).

На компьютерах пользователей в большинстве сетей не используют программу архивации, и мы уделим внимание только серверам. Интересовать нас будут следующие вопросы:

- **Архивация файлов**, то есть обыкновенное помещение файлов и папок в архивный файл.
- **Архивация параметров**, то есть сохранение настроек системы, влияющих на правильную конфигурацию и функционирование всех компонентов системы после восстановления. В Windows 2000/XP/2003 этот набор настроек называется состоянием системы (System state).

Для успешного восстановления сервера следует заранее продумать оба вопроса.

Архивация состояния системы

Как администраторы вы должны знать, какие компоненты системы архивируются в ходе этого процесса. Если посмотреть на нашу сеть, то мы увидим, что её составляют следующие элементы:

- **Компьютеры пользователей**. В состояние системы входят загрузочные файлы запуска системы, база данных COM+ и системный реестр.
- **Сервер**. В состояние системы входят база данных Active Directory (вся доменная база), загрузочные файлы (BOOT.INI, NTLDR, NTDETECT.COM и другие), база данных COM+ (это служба, обеспечивающая взаимодействие компонентов операционной системы и приложений), системный реестр и содержимое папки SYSVOL (объекты групповой политики и сценарии запуска, автоматически реплицируемые между контроллерами домена).

Состояние системы всегда сохраняется целиком, так как его элементы сильно зависят друг от друга. Нельзя архивировать только некоторую его часть (например, реестр).

Таблица 16.1 показывает, что нужно сохранять на компьютерах, выполняющих в сети различные роли, для успешного восстановления критически важных данных.

Что нужно сохранять для успешного восстановления системы *Таблица 16.1*

Данные	Рабочая станция	Рядовой сервер	Контроллер домена
Доменная база данных целиком или ее часть (например, отключенная учетная запись)	нет	нет	Состояние системы
Локальные учётные записи пользователей	Состояние системы	Состояние системы	нет
Операционная система	Состояние системы + содержимое папки %WINDIR%		
Операционная система и приложения	Состояние системы + папка %WINDIR% + все папки, в которых хранятся файлы и данные приложений (Program Files и т.п.)		
Отдельные файлы	Непосредственно файлы или папки с нужными файлами		

Инструменты архивации

В стандартную поставку ОС Windows входит программа архивации. Запустить ее можно либо из главного меню, группа **Все программы → Стандартные → Служебные → Архивация данных**, либо введя в поле **Открыть** диалога **Выполнить** команду **NTBackup**.

Первый раз программа архивации в системах Windows XP/2003 запускается в форме Мастера. Для администратора это не является оптимальным способом, так что разумно будет при первом запуске снять флажок **Всегда запускать в режиме мастера**, нажать кнопку **Отмена** и запустить снова. После этого окно программы будет выглядеть так, как показано на рис. 16.2.

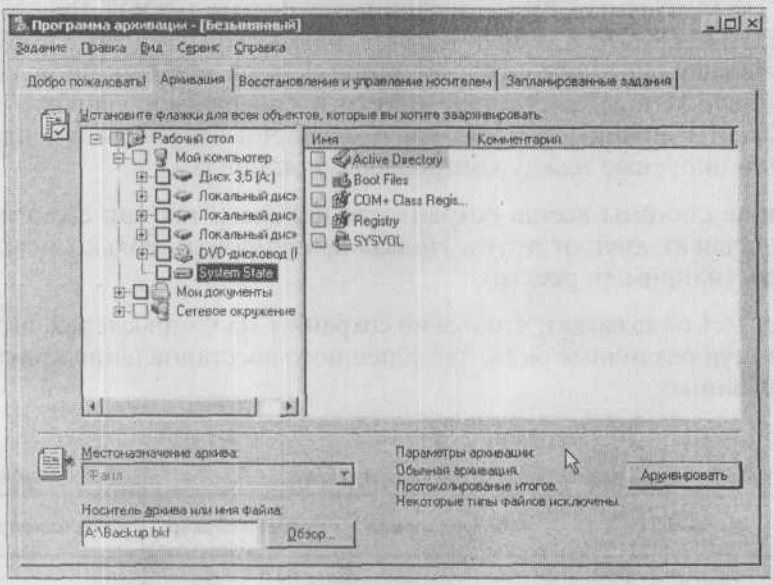


Рис. 16.2. *Элементы состояния системы в Windows Server 2003*

Существует много других программ для архивации системы от других производителей. В случае, если вы намерены приобрести нечто подобное, узнайте, в чём преимущества данного продукта перед интегрированной утилитой Windows. В 80% случаев возможностей стандартной программы архивации вполне хватает.

Стратегии архивации

Сеть существует для пользователей, и регулярная архивация и восстановление системы должны производиться по возможности незаметно для них. Комбинируя типы архивации, можно ускорить либо процесс сохранения данных и настроек, либо процесс восстановления. К сожалению, не оба — одним придется жертвовать ради другого. Различные комбинации типов образуют различные стратегии.

Типов архивации существует пять, и различаются они обработкой атрибута «Архивный» у файлов, выбранных для архивирования. Если вы еще не выполняли архивацию системы, то откройте окно свойств любого файла или папки, и вы увидите, что этот атрибут установлен. При архивации разными способами с ним происходит следующее:

- **Обычный**. Архивируются все выбранные файлы независимо от состояния атрибута, и атрибут снимается.
- **Добавочный.** Из выбранных файлов архивируются те, у которых атрибут установлен, то есть созданные или измененные с момента последней обычной или добавочной архивации. Атрибут «Архивный» снимается.
- **Копирующий**. Архивируются все выбранные файлы независимо от состояния атрибута, и атрибут остается без изменений. Этот способ применяется, когда нужно архивировать отдельные файлы и папки в промежутке между созданием обычных и добавочных архивов, поскольку он не влияет на другие операции архивирования.
- **Разностный**. Из выбранных файлов архивируются те, у которых атрибут установлен, то есть созданные или измененные с момента последней обычной или добавочной архивации, и атрибут остается без изменений.
- **Ежедневный**. Архивируются все файлы, измененные в течение дня. Атрибут «Архивный» не снимается.

При использовании разностной архивации для восстановления файлов и папок требуется наличие последнего обычного и последнего разностного архива. Если использовалась добавочная архивация, то для восстановления нужен как последний обычный, так и все добавочные архивы, созданные после него.

Выбор стратегии архивации зависит от скорости работы всего оборудования, которое участвует в архивации, от доступности данных, от ограничения в сети в процессе архивации, а также от надежности архивируемых серверов и требований пользователей.

В нашей небольшой сети можно ограничиться простейшей стратегией — каждую ночь (в нерабочее время) архивировать все данные. Однако с ростом объема данных может оказаться, что за одну ночь весь этот объем сохранить невозможно, поэтому рассмотрим две другие стратегии.

16.5. Как архивировать?

16.5.1. Стратегия 1 (обычная + добавочная архивация)

Обычная архивация выполняется в течение субботы и воскресенья, а каждую ночь после рабочего дня архивируются только новые и обновленные файлы. Поскольку их сравнительно мало, считаем, что за ночь успеть можно.

Целью администратора в дальнейшем является сделать архивацию автоматической. Мы пойдём этому требованию навстречу и сконфигурируем все необходимые установки для автоматического запуска.

Настройка обычной архивации выходного дня

Постановка задачи: обычная архивация каждую субботу в 23.00 в файл NormalAll.bkf в папку `C:\Backup`, добавочная архивация каждый рабочий день в 23.00 в файлы `Mon.bkf`, `Tue.bkf`, `Wed.bkf`, `Thu.bkf` и `Fri.bkf` в папку `C:\Backup`.

Решение данной задачи выглядит следующим образом:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Запустите программу для архивации данных (NTBackup.exe).
3. Перейдите на вкладку **Запланированные задания** и в календаре нажмите на кнопку **Добавить задание**.
4. Запустится Мастер архивации. Продолжите нажатием кнопки **Далее**.
5. В диалоговом окне **Что следует архивировать** поставьте переключатель в положение **Архивировать все данные на этом компьютере** и нажмите **Далее**.
6. В диалоговом окне **Имя, тип и расположение архивации** задайте размещение `C:\Backup` и название архива «NormalAll». Если папки `C:\Backup` не существует, ее понадобится создать. Потом нажмите на кнопку **Далее**.
7. В диалоговом окне **Тип архива** выберите из списка вид архивации **Обычный** и нажмите **Далее**.
8. На вкладке **Способы архивации** не выбирайте ни один из вариантов и нажмите **Далее**.
9. В диалоговом окне **Параметры архивации** выберите **Заменить существующие архивы** и потом **Разрешить доступ к данным этого архива и всем добавленным на этот носитель архивам только владельцу и администратору**. Нажмите кнопку **Далее**.

10. В диалоговом окне **Когда архивировать** оставьте отмеченным поле **Позже**, в поле **Имя задания** введите «Обычная полная архивация» и нажмите кнопку **Установить расписание**.
11. В диалоговом окне **Запланированное задание** выберите из списка **Назначить задание** — «Еженедельно», в поле **Время запуска** введите время 23.00 и в части **расписание по неделям** выберите только «Сб (суббота)» и «каждую неделю». Потом нажмите кнопку **OK**. В мастере архивации продолжите работу нажатием кнопки **Далее**.
12. В диалоговом окне **Указание учётной записи** введите регистрационное имя (в нашей сети — `ITManager1`) и пароль администратора, у которого есть полномочия для архивирования данных.

Примечание.

Для этой цели было бы с точки зрения безопасности сети разумнее создать новую учётную запись с достаточно сильным паролем и добавить ее в группу `Backup Operators`.

13. Просмотрите введённую информацию и нажмите кнопку **Готово**. В календаре программы архивации появится значок с буквой `N`, означающей вид архивации.

Теперь в системе появилась новое назначенное задание, которое теперь находится полностью в нашем распоряжении. Оно располагается в группе **Панель управления → Назначенные задания.**

Настройка добавочной архивации в рабочие дни

Повторите описанную выше процедуру со следующими необходимыми отличиями:

- Название архива (пункт 6) замените на «Mon».
- В качестве типа архива (пункт 7) выберите **Добавочный**.
- В качестве имени задания (пункт 10) введите «Добавочная архивация Пн».
- В окне **Запланированное задание** (пункт 11) выберите только «Пн».

Повторите эту процедуру четыре раза для остальных рабочих дней с соответствующими исправлениями в именах заданий и файлов. Так образуется 5 запланированных заданий, и в календаре программы архивации каждый рабочий день будет отмечен значком P.

Восстановление данных

Предположим, что архивация какое-то время проходит в полном согласии с поставленными заданиями. Сегодня, к примеру, четверг, последняя

обычная архивация выполнена в прошлую субботу, а последняя добавочная архивация — в среду вечером. Как поступить, если восстановить данные нужно именно сегодня?

В добавочный архив попадают только те файлы, у которых на момент архивации атрибут «Архивный» был установлен, то есть новые или обновленные с момента последней архивации — обычной или добавочной. Значит, для восстановления данных по состоянию на вечер среды нужно последовательно:

1. восстановить данные по состоянию на субботу;
2. применить добавочный архив суббота → понедельник;
3. применить добавочный архив понедельник → вторник;
4. применить добавочный архив вторник → среда.

Если добавочный архив, например, за вторник окажется неисправным (не поддается восстановлению), то все последующие добавочные архивы будут бесполезны, и самыми свежими данными для пользователей окажутся данные по состоянию на понедельник.

Преимуществом этой стратегии является скорость выполнения ежедневных заданий, а недостатком — скорость восстановления.

16.5.2. Стратегия 2 (обычная + разностная архивация)

Как и в предыдущем случае, в выходные архивируются все данные обычным способом. По рабочим дням, в отличие от предыдущей стратегии, архивируются файлы, новые и обновленные по сравнению с вечером субботы, когда выполнялась обычная архивация.

Постановка задачи: обычная архивация каждую субботу в 23.00 в файл `NormalAll.bkf` в папку `C:\Backup`, разностная архивация каждый рабочий день в 23.00 в файлы `Mon.bkf`, `Tue.bkf`, `Wed.bkf`, `Thu.bkf` и `Fri.bkf` в папку `C:\Backup`.

Настройка обычной архивации выходного дня

Настройку обычной архивации выходного дня выполним следующим образом:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Запустите программу для архивации данных (NTBackup.exe).
3. Перейдите на вкладку **Запланированные задания** и в календаре нажмите на кнопку **Добавить задание**.
4. Запустится Мастер архивации. Продолжите нажатием кнопки **Далее**.

5. В диалоговом окне **Что следует архивировать** поставьте переключатель в положение **Архивировать все данные на этом компьютере** и нажмите **Далее**.
6. В диалоговом окне **Имя, тип и расположение архивации** задайте размещение `C:\Backup` и название архива «NormalAll». Если папки `C:\Backup` не существует, ее понадобится создать. Потом нажмите на кнопку **Далее**.
7. В диалоговом окне **Тип архива** выберите из списка вид архивации **Обычный** и нажмите **Далее**.
8. На вкладке **Способы архивации** не выбирайте ни один из вариантов и нажмите **Далее**.
9. В диалоговом окне **Параметры архивации** выберите **Заменить существующие архивы** и потом **Разрешить доступ к данным этого архива и всем добавленным на этот носитель архивам только владельцу и администратору**. Нажмите кнопку **Далее**.
10. В диалоговом окне **Когда архивировать** оставьте отмеченным поле **Позже**, в поле **Имя задания** введите «Обычная полная архивация» и нажмите кнопку **Установить расписание**.
11. В диалоговом окне **Запланированное задание** выберите из списка **Назначить задание** — «Еженедельно», в поле **Время запуска** введите время 23.00 и в части **расписание по неделям** выберите только «Сб (суббота)» и «каждую неделю». Потом нажмите кнопку **ОК**. В мастере архивации продолжите работу нажатием кнопки **Далее**.
12. В диалоговом окне **Указание учётной записи** введите регистрационное имя (в нашей сети — `ITManager1`) и пароль администратора, у которого есть полномочия для архивирования данных.
13. Просмотрите введённую информацию и нажмите кнопку **Готово**. В календаре программы архивации появится значок с буквой N, означающей вид архивации.

Настройка разностной архивации в рабочие дни

Повторите описанную выше процедуру со следующими необходимыми отличиями:

- Название архива (пункт 6) замените на «Mon».
- В качестве типа архива (пункт 7) выберите **Разностный**.
- В качестве имени задания (пункт 10) введите «Разностная архивация Пн».
- В окне **Запланированное задание** (пункт 11) выберите только «Пн».

Повторите эту процедуру четыре раза для остальных рабочих дней с соответствующими исправлениями в именах заданий и файлов. Так образуется 5 запланированных заданий.

Восстановление данных

Предположим, что архивация какое-то время проходит в полном согласии с поставленными заданиями. Сегодня, к примеру, четверг, последняя обычная архивация выполнена в прошлую субботу, а последняя разностная архивация — в среду вечером. Как поступить, если восстановить данные нужно именно сегодня?

В разностный архив попадают только те файлы, у которых на момент архивации атрибут «Архивный» был установлен. Снимает этот атрибут только обычная архивация, но не разностная. Поэтому разностным способом архивируются как действительно новые файлы (обновленные со времени последней разностной архивации), так и относительно новые (новее последней обычной архивации), уже попавшие во вчерашний разностный архив. Значит, для восстановления нужен последний обычный архив и только один разностный архив — последний, то есть в нашем случае за среду. Если он окажется неисправен, то данные удастся восстановить только на тот день, для которого имеется исправный разностный архив.

Недостатком этой стратегии является более медленный по сравнению с добавочной архивацией ежедневный процесс, а преимуществом — быстрота и надежность восстановления (неисправность промежуточных разностных архивов на результате восстановления не скажется).

16.5.3. Управление назначенными заданиями архивации

Если вы посмотрите на свойства созданных программой архивации назначенных заданий, вы обнаружите, что каждое задание представляет собой запуск утилиты `ntbackup.exe` с аргументом — именем файла. Обратите внимание на размещение этого файла: оказывается, он является частью профиля пользователя! Это не слишком удачное место, потому что администратор компьютера может в любой момент удалить профиль, а вместе с ним все нужные файлы.

Разумнее переместить эти файлы в другое место вне профиля (например, в папку `C:\PlanBackup`). Не забудьте только предоставить пользователю, от имени которого должно запускаться назначенное задание, доступ к этой папке на чтение.

16.5.4. Восстановление Active Directory

Для полноты и практического использования приведённых стратегий нужно добавить немного информации о восстановлении службы каталогов. Архивируется она как составная часть Состояния системы, которое всегда сохраняется и восстанавливается как единое целое.

В этом параграфе мы рассмотрим действия по восстановлению службы каталогов на случай, если сервер SRVR001 полностью вышел из строя, а затем рассмотрим восстановление Active Directory в среде домена с несколькими контроллерами.

Восстановление Active Directory в домене с одним контроллером (неавторизованное восстановление)

Для восстановления службы каталогов после аппаратного сбоя нам понадобится файл с архивом состояния системы на контроллере домена. Считаем, что он у нас есть. Тогда выполните следующие действия:

1. Перезагрузите SRVR001 в режиме восстановления службы каталогов (при запуске системы нажмите клавишу F8 и выберите этот режим). Для контроллера домена это единственный режим, в котором служба каталогов не стартует. Но под каким именем регистрироваться, если локальных учетных записей на контроллере домена не существует, а доменные недоступны, потому что домен сейчас не работает? В главе 7, устанавливая домен, вы вводили пароль администратора для режима восстановления. Сейчас вам нужно зарегистрироваться под именем Администратор (Administrator) и ввести этот пароль. Если вы его забыли, то восстановить домен не удастся никак.
2. Запустите программу архивации (**Пуск → Выполнить**, ntbackup) и перейдите на вкладку **Восстановление и управление носителем**.
3. Из списка в правой части окна выберите метку архива и установите флажок **Состояние системы**. Из списка **Восстановить файлы в** выберите «Исходное размещение». Переключатель **Если файл уже существует** установите в положение **Всегда заменять имеющийся файл**. Нажмите кнопку **Восстановить**. Это приведет к перезаписи текущего состояния системы.
4. После успешного восстановления вам будет предложено перезагрузить компьютер — нажмите **Да**. База данных Active Directory будет обновлена после перезагрузки.

Описанные действия следует выполнять в одном из двух случаев:

- Восстановление домена с одним контроллером;
- Полное восстановление контроллера в домене с несколькими контроллерами.

Если же в вашем домене есть несколько контроллеров, синхронизирующих данные активного каталога между собой в ходе репликации, а вы хотите откатить небольшое изменение (например, ошибочное удаление доменной учетной записи), то описанный способ действий для этого непригоден. В этом случае следует выполнить авторизованное восстановление.

Авторизованное восстановление Active Directory

Пусть у нас есть два контроллера домена: SRVR001 и SRVR002. Данные доменной базы можно менять на любом из контроллеров, и в ходе последующей репликации это изменение распространяется на все остальные.

Предположим, что кто-то из администраторов по ошибке удалил доменную учётную запись пользователя Shop2. В системном журнале записано, что это случилось в понедельник в 11:25. К восстановлению учётной записи может привести только восстановление Active Directory. Вы обнаружили, что последняя архивация состояния системы на домене SRVR001 состоялась в воскресенье, в 23:47.

Поскольку безразлично, на каком из контроллеров домена выполнять восстановление, выбирайте тот из них, недоступность которого во время восстановления меньше повлияет на работу пользователей сети — желательно тот, который не выполняет других серверных ролей. Выберем для примера SRVR001.

Что получится, если вы восстановите базу данных Active Directory неавторизованным способом? Различие между двумя доменными базами данных на серверах SRVR001 и SRVR002 будет заключаться только в одной учётной записи. Процесс репликации сравнит временные отметки, чтобы определить, какое изменение распространять на другие контроллеры.

Информация о существовании учётной записи `Shop2` на сервере SRVR001 будет иметь отметку времени «Воскресенье, 23:47». Информация о несуществовании учётной записи `Shop2` на сервере SRVR002 будет отмечена текущим временем (например «Понедельник, 16:20»). Поскольку эта база данных новее, через некоторое время она и будет реплицирована на SRVR001, то есть учётная запись `Shop2` снова исчезнет из домена.

Обычно авторизованному восстановлению подлежит не вся база данных, а отдельные объекты или поддеревья — например, единственная учетная запись `Shop2`. После этого нужно обновить метку времени в соответствии с текущим временем.

1. Выполните первые три шага, описанные в предыдущем параграфе, а на четвертом шаге откажитесь от немедленной перезагрузки — нажмите **Нет**.

2. После этого запустите командную строку и введите команду **ntdsutil**.
3. Далее введите следующие команды (считаем, что учётная запись Shop2 находилась в контейнере `Users`):

```
authoritative restore
restore subtree CN=Shop2, CN=Users, DC=study, DC=local
quit
quit
exit
```

4. Теперь перезагрузите SRVR001.

Если нужно восстановить всю доменную базу данных авторизованным способом, то после запуска утилиты **ntdsutil** введите следующую последовательность команд:

```
authoritative restore
restore database
```

В диалоговом окне нажмите на кнопку **OK** и потом на кнопку **Да**.

16.6. Теневое копирование

Теневое копирование — это новая функция, появившаяся в Windows XP и Windows Server 2003 и делающая возможной архивацию открытых файлов, что было немыслимо в предыдущих версиях Windows (в частности, Windows 2000).

Когда приходится архивировать открытые файлы? Пусть, например, на одном из рабочих мест вашего предприятия все еще работает старинная бухгалтерская программа. Собственного механизма архивации она не имеет и данные способна держать только на локальном компьютере. Об архивировании ее базы данных придется думать администратору, то есть вам.

Во время архивирования этих файлов по сети компьютер бухгалтера должен быть включен, но программа работать не должна, чтобы файлы не оставались открытыми. Но эта программа написана как автоматизированное рабочее место, стартует при включении компьютера и завершается при его выключении, и вам остается только проклинать ее автора.

Выходом из этой ситуации станет установка на рабочее место бухгалтера Windows XP Professional (считаем, что привычная программа будет работать и под этой операционной системой). После этого вы сможете архивировать все рабочие файлы этой программы без оглядки на то, завершена она или нет.

Теневое копирование и общие папки

Теневая копия томов используется ещё в одном случае. С помощью неё можно вернуться к предыдущей версии файла в разделяемой папке на сервере. Управление версиями документов мы здесь рассматривать не будем. Гораздо важнее следующий факт. В предыдущих версиях Windows (включая Windows 2000) удаление файла из общей папки по сети приводило к его безвозвратной потере — он не оставался даже в Корзине. А в ОС Windows Server 2003, удалив файл, вы сможете восстановить его предыдущую версию, которая может оказаться идентична текущей.

Можете сами сравнить трудоемкость восстановления документа из архивов в системе Windows 2000 с возможностью вернуться к предыдущей версии документа в системе Windows Server 2003. На практике именно эта функция является самым веским доводом для перевода файловых серверов с Windows 2000 на Windows Server 2003.

По умолчанию теневое копирование общих папок выключено. Включается оно на сервере для раздела, на котором физически расположены общие папки. Это должен быть раздел с файловой системой NTFS.

1. Зарегистрируйтесь на SRVR001 как администратор. Откройте окно свойств диска C:.
2. Перейдите на вкладку **Теневое копирование**. Вы увидите, что эта функция отключена.
3. Нажмите кнопку **Параметры** и отредактируйте свойства текущего раздела. Вы можете указать, как часто будет копироваться раздел (по умолчанию два раза в день) и какое место на диске отводится под копии. Рекомендуется оставить значения по умолчанию. Закройте диалоговое окно нажатием кнопки OK.
4. Нажмите кнопку **Разрешить** и в следующем диалоговом окне подтвердите своё решение нажатием кнопки **Да**.

Сразу после этого начнется создание первой копии раздела. Информация об этом действии в форме даты и времени отобразится в нижней части окна.

Примечание.

Не обязательно копировать раздел на тот же самый физический диск. Если у вас установлено несколько физических дисков, вы существенно повысите производительность дисковой подсистемы, направив копию на другой диск. Единственное условие — этот диск должен быть отформатирован в файловой системе NTFS.

Организация теневого копирования на рабочей станции

Клиентские компьютеры под управлением Windows XP Professional не могут использовать функцию теневого копирования сразу. Сначала на них нужно установить клиентское программное обеспечение. Установочный файл `TWCLI32.MSI` находится на сервере (под управлением Windows Server 2003) в папке `%SYSTEMROOT%\system32\clients\twclient\x86`.

1. Зарегистрируйтесь на PC001 как администратор.
2. Запустите Проводник и в адресной строке введите путь `\\SRVR001\c$\windows\system32\clients\twclient\x86\twcli32.msi`. Установится клиент Previous Versions Client.

Клиенты для операционных систем Windows 2000 Server с установленным пакетом обновления SP3 и далее, Windows 2000 Professional и Windows 98 можно скачать с сайта Microsoft по адресу `http://www.microsoft.com/windowsserver203/downloads/shadowcopyclient.mspx`.

Для операционных систем Windows NT 4.0 такого клиента не существует. Для систем ниже, чем Windows XP, клиентскую программу нужно установить как на клиентский компьютер, так и на сервер с системой Windows Server 2003.

Применение теневого копирования

Чтобы воспользоваться благами теневого копирования:

1. Зарегистрируйтесь на PC001 как рядовой пользователь (например, `Shop3`).
2. Откройте папку своего подразделения в общем хранилище документов (глава 12) (`\\SRVR001\Библиотека\Продажи`).
3. Отобразите свойства любого файла (лучше текстового). Перейдите на вкладку **Предыдущая версия**. С момента установки клиента теневого копирования ни одной предыдущей версии еще не создавалось, поэтому список пуст.
4. Откройте файл, отредактируйте его и сохраните под тем же именем.
5. *Повторите* п.3. Теперь на вкладке **Предыдущая версия** вы увидите предыдущую версию файла с датой ее создания.
6. Вы можете просмотреть ее, нажав кнопку **Отобразить**. Копия документа предназначена только для чтения, и переименовать и сохранить ее невозможно. Чтобы восстановить предыдущую версию под другим именем, нужно сначала скопировать ее в другое место, нажав кнопку **Копировать.**

Если вы по ошибке удалили файл из общей папки и хотите его восстановить, поступайте следующим образом:

1. С клиентского компьютера отобразите свойства папки, в которой был документ, и перейдите на вкладку **Предыдущая версия**.
2. Нажмите кнопку **Отобразить** и просмотрите содержимое предыдущей версии документа. Если оно вас устраивает, создайте новый документ и скопируйте в него содержимое через буфер обмена.

Если вы ошибочно отредактировали и сохранили документ, то можете восстановить его правильную версию, нажав кнопку **Восстановить** на вкладке **Предыдущая версия.**

Таким образом, функция теневого копирования помогает пользователям быстро восстановить их документы, находящиеся в разделяемых папках, в следующих случаях:

- при неумышленном удалении файлов;
- при неумышленном изменении содержания файлов (использование команды **Сохранить** вместо **Сохранить как**);
- при повреждении файлов.

Обратите внимание, что копируется весь раздел, а не только папки, к которым на момент копирования открыт сетевой доступ. Это значит, что, если после создания копии вы предоставите доступ к новой папке, предыдущие версии ее файлов будут доступны пользователям с момента открытия доступа.

16.7. Итоги

Вы должны хорошо подготовиться к внезапному выходу сервера из строя. Неполадки могут поджидать вас как со стороны оборудования, так и со стороны программного обеспечения. Вы должны продумать свои действия на случай аппаратных и программных сбоев, ошибок пользователей и администраторов заранее, уже в ходе развертывания сети.

Системы Windows XP Professional и Windows Server 2003 содержат функцию отката к предыдущей версии драйвера. Это очень полезная функция, которая может помочь вам справиться с неполадками оборудования в течение нескольких секунд. Чтобы проблемы с драйверами возникали реже, никогда не устанавливайте неподписанные драйвера.

Если компьютер не загружается, попытайтесь запустить его в безопасном режиме или в режиме последней удачной конфигурации. Если ни один из этих способов не помогает, проблема может заключаться в повреждении одного из загрузочных файлов. Свои подозрения вы можете подтвердить, загрузившись в режиме протоколирования. В этом режиме в папке `%SYSTEMROOT%` создается файл с названием `NTBTLOG.TXT`, который вы потом сможете просмотреть с помощью Консоли восстановления. Это ути-

лита с интерфейсом командной строки, позволяющая читать и записывать данные в разделы с файловой системой NTFS. Консоль восстановления можно запустить с установочного компакт-диска или заранее установить на компьютер, после чего она станет одним из вариантов загрузки.

Пользователь может по ошибке удалить или неверно отредактировать файл в сетевой папке. Для облегчения восстановления файла предназначена функция теневого копирования разделов, позволяющая вернуться к одной из предыдущих версий файла. Теневая копия раздела по умолчанию создается два раза в день, а старые версии удаляются тогда, когда на диске, отведенном для копий, больше нет места.

Функция теневого копирования на сервере реализована средствами ОС Windows Server 2003, а на рабочей станции под управлением Windows XP Professional, Windows 2000 и даже Windows 98 должен быть установлен специальный клиент.

Со стороны оборудования вы можете ожидать отказа жёсткого диска. Система Windows Server 2003 поддерживает объединение дисков в массивы RAID 0 (необходимо два физических диска) и RAID 5 (необходимо не менее трех физических дисков, возможно до 32). Клиентские операционные системы не поддерживают массивы RAID.

Описание способов повышения надежности сети могло бы занять целую книгу, но и эта глава даст вам достаточно информации для поддержания сетевой среды вашего предприятия в рабочем состоянии.

Состояние сети

На сервере SRVR001 установлена Консоль восстановления. При включении компьютера она отображается как один из вариантов загрузки.

Мы выбрали стратегию резервного копирования (архивации) нашей сети и назначили задания, которые будут выполнять архивацию автоматически. Хранить архивы безопаснее на магнитных лентах. Если же вы архивируете на жесткий диск, то категорически не рекомендуется использовать для этого системный диск.

На сервере включена функция теневого копирования, а на рабочих станциях установлены соответствующие клиенты. Копирование включено для всех разделов, где есть разделяемые папки, и для хранения копий выделен отдельный физический диск.

Видите, как увеличиваются требования к количеству жестких дисков на сервере?

Глава 17 Групповые политики. Управление группой компьютеров пользователей

После входа в систему и создания нового профиля у пользователей есть в распоряжении почти все, что может предоставить операционная система Windows XP Professional. Кроме того, что в рабочее время они должны пользоваться приложениями, нужными им для работы, они могут играть в игры, которые являются стандартной частью системы или ежедневно забавляться тем, какую картинку им сделать фоновым рисунком рабочего стола.

Более шустрые приносят дискеты или компакт-диски с приложениями, не требующими установки, и развлекаются в рабочее время с ними. А самые шустрые забивают свой компьютер музыкальными хитами и новинками видео.

А теперь посмотрите на эту ситуацию глазами руководства и владельцев компании. Они бы хотели, чтобы пользователи были максимально ограничены в своих действиях. Тем, кто до сих пор не может выбрать рисунок рабочего стола, установленные параметры не дадут что-либо изменить, для тех же, кто обожает запускать приложения с диска CD-ROM, есть ограничения, которые позволяют запускать только определённые программы.

Возможностей в системах Windows XP Professional и Windows Server 2003 предостаточно. В этой главе мы рассмотрим несколько главных областей и так настроим пользовательские компьютеры, что это понравится руководству и в то же время не будет мешать нормальной работе пользователей.

17.1. Инструменты управления компьютерами пользователей. Групповые политики

Что такое групповая политика?

Задачей каждого администратора является управлять доверенной ему группой как можно более эффективно. Это значит посвящать управлению как можно меньше времени и усилий.

Успешный администратор — это не тот, который целый день не знает, куда бы ему ещё сунуть свой нос, чтобы удержать сеть на плаву. Такой администратор чаще всего только тормозит работу пользователей. Успешный администратор — тот, кто точно представляет, как выглядят компьютеры пользователей, знает, что никакие лишние функции не отвлекают пользователей от работы, уверен, что документы организации находятся в безопасности, и у которого есть ещё время подумать над развитием сети, изучить новые технологии и поэкспериментировать в своей тестовой лаборатории.

Эта глава написана для того, чтобы показать администраторам, с помощью каких средств они будут способны эффективнейшим способом управлять группой компьютеров пользователей. Для установки большинства параметров, которые вы хотите применить в сети, хватает одного средства. Но, чтобы возможности этого средства были использованы по максимуму, в его «услугах» необходимо разобраться.

Групповые политики (Group Policy) — это часть технологии IntelliMirror, появившейся с приходом системы Windows 2000. Оснастка **Групповые политики** продолжает идеи Диспетчера учетных записей в системе Windows NT 4.0, но по сравнению с ним более функциональна и проще в понимании и управлении. Групповая политика является именно тем средством, которое служит для упрощения управления компьютерами пользователей.

К сожалению, у этого средства есть и ограничения. Политики применяются только к компьютерам под управлением Windows XP Professional, Windows Server 2003 и Windows 2000, являющимся членами домена. Если в сети появился компьютер с иной операционной системой, ему необходимо уделить особое внимание, поскольку Групповая политика на него распространяться не будет.

Обзор оснастки Групповая политика.

Книг и статей на эту тему написано много, и, вместо того чтобы повторять их материал здесь, я сосредоточусь на главных особенностях, а остальное

продемонстрирую на примере нашей учебной сети. В предыдущих главах мы уже несколько раз пользовались оснасткой **Групповая политика**, так что многое покажется вам знакомым.

Средство **Групповая политика** есть в каждом компьютере с системой Windows 2000 и выше, и на локальном компьютере его можно запустить двумя способами:

- Запуском пустой консоли MMC и добавлением модуля оснастки с названием Групповая политика.
- Введением команды **gpedit.msc** в командной строке или в окне **Пуск → Выполнить**.

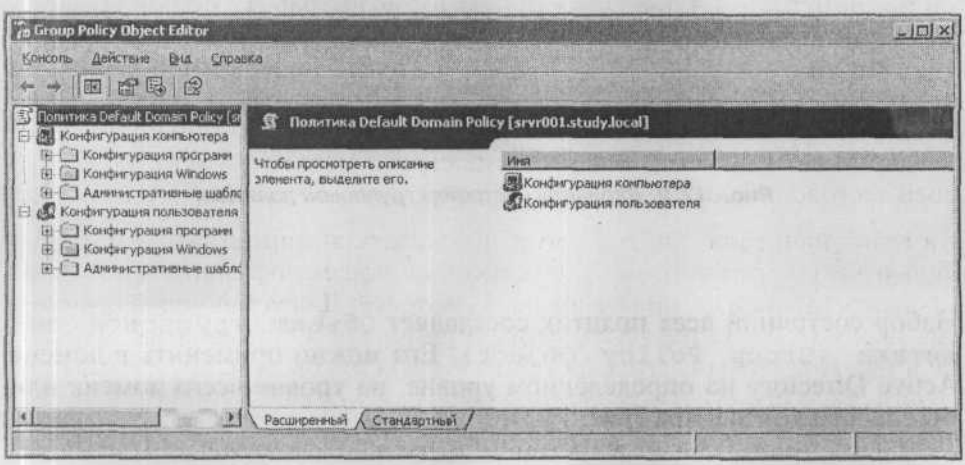


Рис. 17.1. *Оснастка Групповая политика, запущенная на компьютере с системой Windows Server 2003*

Политики (всего их более 700) сгруппированы в две ветви: **Конфигурация компьютеров** и **Конфигурация пользователей**. Все политики, заданные в части **Конфигурация компьютера**, применяются к компьютеру независимо от того, какой пользователь за ним работает. Политики, заданные в части **Конфигурация пользователя**, применяются к учетной записи пользователя независимо от того, за каким компьютером он зарегистрирован. Некоторые политики присутствуют в обеих ветвях, другие — только в одной.

Почти каждая политика может находиться в одном из трех состояний (рис. 17.2):

- Не задано (не определено).
- Включено.
- Отключено.

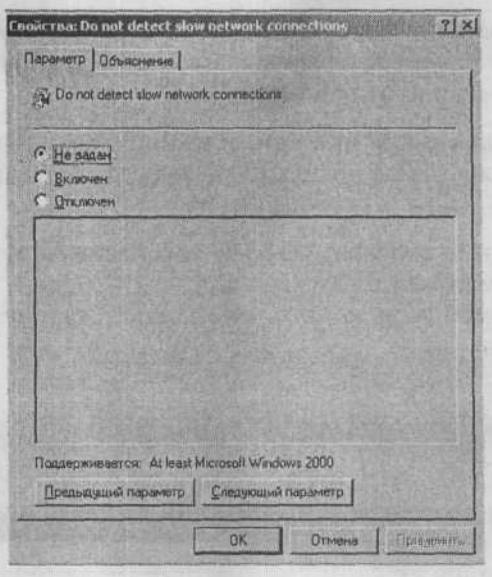


Рис. 17.2. *Варианты настройки групповой политики*

Набор состояний всех политик составляет `Объект групповой политики (Group Policy Object)`. Его можно применить в домене Active Directory на определённом уровне: на уровне всего домена или отдельного контейнера (рис. 17.3).

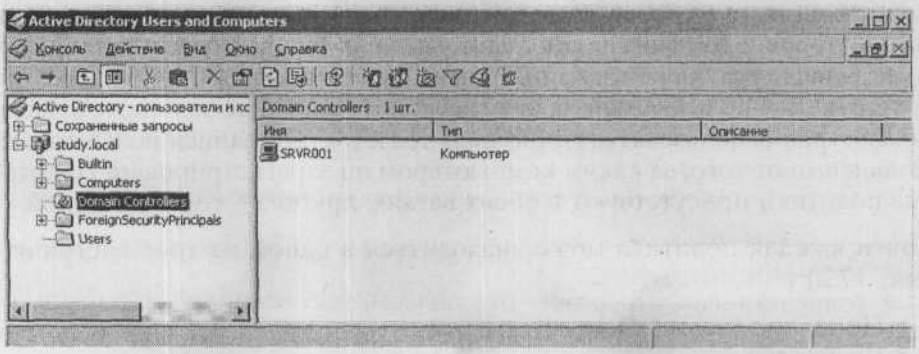


Рис. 17.3. *Иерархическая структура домена Active Directory*

Примеры применения объекта групповой политики

Если вы создадите объект групповой политики и примените его на уровне домена (study.local), то политики, входящие в ветвь **Конфигурация компьютера,** повлияют на все компьютеры в домене, а политики в ветви **Конфигурация пользователя** повлияют на всех пользователей домена. По умолчанию такой объект уже создан. Он называется Default Domain Policy (доменная политика по умолчанию), и в этой книге мы уже с ним несколько раз сталкивались и даже корректировали. Его основным назначением является настройка параметров учётных записей пользователей домена.

Если вы создадите другой объект групповой политики и примените его на уровне Domain Controllers (который содержит только учётные записи контроллеров домена), то политики из ветви **Конфигурация компьютера** будут применены только к учётным записям компьютеров в данной организационной единице (то есть только на контроллерах домена), а политики в ветви **Конфигурация пользователя** не будут применены вообще, поскольку в контейнере `Domain Controllers` нет никаких учётных записей пользователей. По умолчанию такой объект уже создан, и называется он Default Domain Controllers Policy. Он служит для начальной настройки контроллера домена.

В иерархической структуре домена Active Directory имеет место такое понятие как наследственность. Это означает, что политики из объекта, примененного к вышестоящему контейнеру, автоматически применяются и к подчинённым контейнерам, если включен режим наследования.

Особое положение занимают локальные объекты групповой политики. Они применяются только к локальному компьютеру и локальным пользователям.

Если удалить объект групповой политики, то все политики вернутся в состояние по умолчанию. То же произойдет в случае перемещения учётной записи пользователя в иерархии Active Directory на другое место, где на него никакой объект групповой политики не действует.

В следующих частях этой главы мы подробно рассмотрим отдельные политики и варианты их настройки.

Главные ветви групповой политики

Все политики в объекте разделены на несколько областей:

- **Конфигурация программ.** Эта область обеспечивает установку, обновление и удаление программного обеспечения. Подробнее о ее практическом использовании вы узнаете из глав 18 и 20, посвященных установке приложений и пакетов обновления

- **Конфигурация Windows.** Этот очень важный раздел обеспечивает безопасность компьютеров. Он состоит из большого количества политик (около 150), касающихся паролей, аудита, конфигурации членства в группах, безопасности ключей реестра и файлов, безопасности IP-протокола и многих других. Дальнейшую информацию о настройке безопасности вы найдёте в главе 22.
- **Административные шаблоны.** Эта область содержит больше всего политик, управляющих возможностью запуска и конфигурирования приложений, запретами или разрешениями изменять системные файлы и т.п. Некоторые их этих политик мы уже упоминали в предыдущих главах.

17.2. Иерархическая структура Active Directory

Домен Active Directory имеет иерархическую структуру. Он является первым доменом подобного рода от компании Microsoft. Иерархическое строение домена значительно облегчает работу администратора, одновременно увеличивая гибкость настройки различных параметров в сети.

Например, политики, которые так или иначе должны касаться всех пользователей в домене, можно сконфигурировать в объекте на уровне домена, параметры же, касающиеся отдельных подразделений, могут быть помещены в объект, применяемый на уровне конкретной организационной единицы, соответствующей данному подразделению.

Иерархию домена образуют контейнеры типа «организационная единица» (OU, organisation unit). Если сопоставить организационным единицам домена подразделения нашего предприятия, то мы получим возможность по-разному конфигурировать компьютеры сотрудников, работающих в разных отделах. Скажем, работникам склада совершенно не обязательно иметь доступ к Панели управления вообще; сотрудникам отдела продаж можно разрешить доступ к апплетам **Клавиатура** и **Язык и региональные стандарты**, руководству же можно разрешить доступ ко всей Панели управления.

Понятно, что возможность гибкого управления отделами зависит от правильного разбиения активного каталога на организационные единицы. Нужно продумать размещение учетных записей пользователей и компьютеров по организационным единицам так, чтобы не пришлось каждый день перестраивать структуру.

Важнее всего структурировать верхний уровень. Для географически распределенных предприятий уместно будет сопоставить организационные единицы верхнего уровня филиалам в разных городах, а для небольшого

предприятия они могут совпадать с делением на отделы. Для нашего учебного предприятия Study применим второй подход.

Чтобы создать организационную единицу, запустите от имени администратора консоль **Active Directory — пользователи и компьютеры** и из контекстного меню контейнера study.local выберите команду **Создать → Подразделение.** Введите имя новой организационной единицы. Вы всегда сможете его сменить, причем это никак не повлияет на работу пользователей.

Создайте организационные единицы для наших подразделений IT, Marketing, Shop, Store и Managers (рис. 17.4).

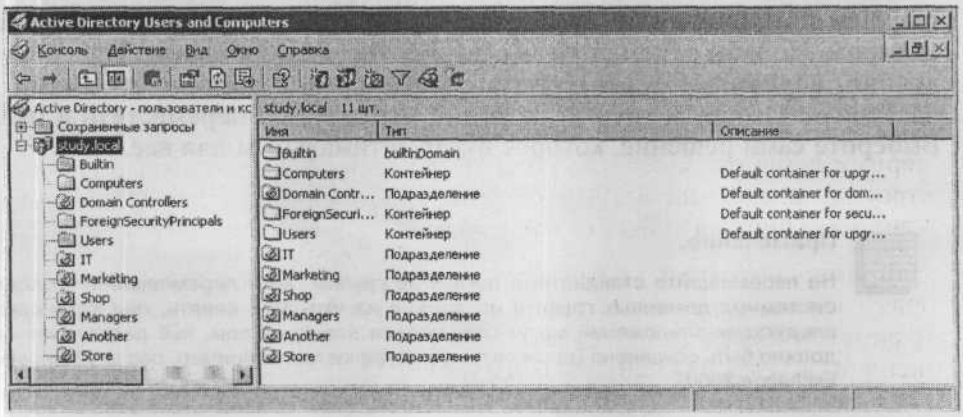


Рис. 17.4. *Первый уровень структуры активного каталога в сети предприятия Study*

Теперь нужно разместить по соответствующим подразделениям учетные записи пользователей. На примере отдела продаж:

1. Запустите консоль **Active Directory — пользователи и компьютеры.**
2. В левом подокне разверните контейнер `Users`. В правом окне выделите все учетные записи пользователей из отдела продаж (Shop1 ... Shop5), щелкая по ним при нажатой клавише Ctrl. Щелкните по выделенной группе правой кнопкой мыши и выберите из контекстного меню команду **Переместить**. Отобразится диалоговое окно со структурой домена Active Directory.
3. В появившемся диалоговом окне со структурой домена щелкните по контейнеру Shop и нажмите кнопку **OK**.
4. Не забудьте переместить и шаблоны учётных записей.

Примечание.

Если вы работаете в ОС Windows XP Professional или Windows Server 2003, то перемещать объекты в окне консоли **Active Directory — пользователи и компьютеры** можно при помощи протаскивания мышью. В Windows 2000 это делается только через команду меню.

Учётные записи компьютеров оставьте в контейнере `Computers`. Речь идёт об исходном контейнере, в котором учётные записи создавались в процессе добавления компьютеров в домен.

Организационную единицу `Domain Controllers` лучше не трогать, иначе вы можете столкнуться с огромными проблемами.

Созданные локальные домены и глобальные группы вы можете оставить в текущем контейнере или переместить их в подходящие организационные единицы. Но я бы рекомендовал оставить текущее состояние. Наверное, лучшим вариантом будет создать особую организационную единицу, названную Groups и группы, которые мы создали, переместить в неё. Выберите сами решение, которое будет оптимальным для вас.

Примечание.

Не перемещайте стандартные доменные группы. Хотя перемещение текущих системных доменных групп и не должно на что-либо влиять, при установке следующих приложений могут создаваться новые группы, чьё расположение должно быть сохранено (такая ситуация встречается, например, после установки Exchange 2000).

Теперь домен подготовлен к тому, чтобы мы могли начать настраивать и применять политики. Начнем с сокрытия всех файлов, не нужных пользователям для их повседневной работы, чтобы они не отвлекались.

17.3. Сокрытие ненужных файлов

17.3.1. Что не нужно пользователям?

Например, некоторые команды в меню **Пуск**. Нужна ли в ней пользователям команда **Выполнить**? Если да, то речь будет идти об исключении из правил. А папки «Мои рисунки» и «Моя музыка»? А нужно ли им настраивать себе что-либо средствами Панели управления? Или эту команду можно оставить, но с ограниченным набором апплетов?

17.3.2. Как настроить групповые политики, скрывающие команды меню

Настройка политики сокрытия

Рекомендуется применять эти политики сразу же после установки домена, чтобы пользователи быстрее примирились с ограничением своих возможностей (или никогда не узнали о том, чего лишены). Также обязательно посоветуйтесь с руководителями отделов — их авторитет вам понадобится, если пользователи все-таки придут жаловаться.

Сейчас мы настроим политику сокрытия, применяемую ко всему домену, а для отдельных подразделений потом можно будет изменить некоторые параметры, применив политику на уровне организационной единицы.

1. Зарегистрируйтесь на PC001 как администратор. Запустите консоль **Active Directory — пользователи и компьютеры.**
2. Откройте окно свойств домена `study.local` и перейдите на вкладку **Групповые политики**.
3. Нажмите кнопку **Создать**. Появится новый объект групповой политики. Дайте ему имя «Hide unnecessary files» (сокрытие ненужных файлов).
4. Щелкните по новому объекту. Запустится оснастка **Групповая политика**.
5. Перейдите в раздел **Конфигурация пользователя\Административные шаблоны\Панель задач и меню Пуск**. Установите значения политик этого раздела согласно таблице 17.1.

Политики по отношению к главному меню *Таблица 17.1*

Политика	Значение	Примечания
Удалить значок «Мои рисунки» из главного меню	Включено	Эта политика действует только на компьютерах с Windows XP Professional. В главном меню Windows 2000 этих значков нет
Удалить значок «Моя музыка» из главного меню	Включено	
Удалить значок «Сетевое окружение»	Включено	
Удалить контекстные меню...	Включено	
Запретить изменение параметров панели задач и главного меню	Включено	
Отключить сокращенные меню	Включено	По умолчанию Windows автоматически скрывает долго не используемые команды меню. Некоторые пользователи беспокоятся и звонят администратору
Удалить всплывающие подсказки...	Включено	Действует только для Windows XP Professional
Удалить имя пользователя из главного меню	Включено	Чтобы злоумышленник не подсмотрел. Действует только для Windows XP Professional

6. Перейдите в раздел **Конфигурация пользователя\Административные шаблоны\Рабочий стол**. Установите значения политик этого раздела согласно таблице 17.2.

Политики по отношению к рабочему столу *Таблица 17.2*

Политика	Значение	Примечания
Убрать значок «Сетевое окружение»	Включено	
Запретить изменять путь папки «Мои документы»	Включено	Вы переадресовали эту папку на сервер, и пользователю нужно помешать переложить ее в неизвестное вам место
Не сохранять параметры настройки при выходе	Включено	Если пользователь нечаянно перетащил панель задач туда, откуда сам не вытащит, то он сможет помочь себе перерегистрацией
Удалить мастер очистки рабочего стола	Включено	Чтобы не пропали ярлыки, которые пользователь не трогал 60 дней

7. Перейдите в раздел **Конфигурация пользователя\Административные шаблоны\Система**. Включите политику «Не запускать указанные приложения Windows» и перечислите игры freecell.exe, spider.exe, winmine.exe, pinball.exe, sol.exe, mshearts.exe и редактор реестра regedit.exe.

Теперь зарегистрируйтесь как рядовой пользователь и попытайтесь запустить `regedit`. Вы увидите сообщение о том, что запуск этого приложения запрещен администратором.

Здесь есть одно «но». Поскольку эти политики сконфигурированы на уровне домена, они будут воздействовать на всех доменных пользователей, в том числе и на администраторов. Значит ли это, что администраторы не смогут полноценно работать? Пока это так, но мы этот вопрос потом решим.

Активация политики в отношении пользователей

После входа в систему с компьютера PC001 мы проверили, что все параметры установлены успешно. На практике, однако, может случиться, что в то время, когда вы будете настраивать групповую политику, некоторые пользователи могут войти в систему и работать. Не исчезнут ли у них скрываемые файлы прямо перед носом?

Чтобы ответить на этот вопрос, нужно понять, когда и как политики применяются к конкретному пользователю. Далее в этом параграфе мы считаем, что без сети регистрация пользователя не происходит (включена политика **Всегда ожидать инициализации сети** в ветви **Конфигурация компьютера\Административные шаблоны\Система\Вход в систему** объекта

Default Domain Policy). В Windows 2000 это настройка по умолчанию, а в Windows XP Professional нужно установить эту политику вручную, как мы сделали в предыдущих главах.

Когда активируются политики, входящие в раздел **Конфигурация пользователя**:

- При выходе и входе пользователя в систему (при каждой регистрации компьютер опрашивает контроллеры доменов о наличии объектов групповой политики, которые применяются к пользователю, и применяет их). Только после этого отображается рабочий стол пользователя.
- К пользователям, уже зарегистрировавшимся в системе, политики будут применены постепенно, в течение двух часов. Этот интервал предназначен для того, чтобы сотни рабочих станций не обращались к контроллерам домена одновременно, перегружая тем самым сеть.
- Когда на клиентском компьютере (под управлением Windows XP Professional или Windows Server 2003) будет запущена утилита командной строки GPUPDATE. В Windows 2000 вместо нее служит команда

```
secedit /refreshpolicy user_policy /enforce
```

Если два часа (90 минут плюс-минус случайная величина от 1 до 30 минут) вас не устраивают, то можете применить политику **Интервал обновления групповой политики для пользователей** в разделе **Конфигурация пользователя\Административные шаблоны\Система\Групповая политика.** Установите там постоянную и случайную части нового интервала.

17.3.3. Сколько объектов групповой политики создавать?

Чтобы ограничить пользователей, у вас было две возможности: либо изменить состояние политик по умолчанию в объекте Default Domain Policy, либо создать и применить новый объект. Как поступать, зависит от конкретных условий на вашем предприятии.

Доводы в пользу одного объекта

Каждый объект представляет собой набор файлов и папок общим объёмом 1,66 Мб. Если на сервере уже не хватает места, то несколько объектов групповой политики держать на нем невыгодно. Кроме того, чем больше объектов групповой политики существует для пользователя, тем больше времени при его входе в систему потребуется для того, чтобы применить их по очереди.

Доводы в пользу нескольких объектов

Если вы измените объект политик по умолчанию (Default Domain Policy), то значения в нем уже не будут соответствовать настройкам по умолчанию и его название потеряет смысл. Вернуться к исходным значениям будет непросто, если не документировать тщательнейшим образом, что именно было изменено.

Другая причина — гибкость управления. Вы могли бы создать отдельный объект для ограничения функциональности главного меню, отдельный — для ограничения рабочего стола и т.п. и применять некоторые из этих объектов на уровне подразделений, а другие — на уровне всего домена.

17.3.4. Администраторские привилегии и как их не потерять

Настройка локальных администраторских привилегий

Когда вы включаете компьютер под управлением Windows XP Professional в домен, вам больше не обязательно знать пароль локального администратора, потому что теперь вы можете управлять этим компьютером как администратор домена. Это возможно благодаря тому, что группа `Domain Admins` по умолчанию входит в локальную группу `Administrators`.

Когда вы убираете компьютер из домена, группа `Domain Admins` из локальной группы `Administrators` удаляется. Но удалить ее может вручную пользователь, если он знает пароль локального администратора или его доменная учетная запись тоже (индивидуально, а не благодаря членству в группах) входит в локальную группу `Administrators`. Для администратора домена этот риск неприемлем, но, к счастью, применение подходящей групповой политики позволяет свести его на нет.

Другим применением для групповой политики, о которой пойдет речь в этом параграфе, является следующая задача. Допустим, вам нужно на сотне рабочих станций под управлением Windows XP Professional добавить в реестр, в ключ HKEY_LOCAL_MACHINE, некоторый подключ. Право на это действие есть у локальных администраторов, которыми вы являетесь благодаря членству в группе `Domain Admin`, но выполнять его самому у вас нет времени. А если нанять на несколько дней контрактника для выполнения этой работы, то пришлось бы раскрыть ему пароли локальных администраторов. Пришлось бы, если бы не было политики **Группы с ограниченным доступом** (ветвь **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности**).

Членами такой группы являются только те учетные записи и группы, которые вы явно укажете. Так, в группу локальных администраторов можно

включить только локальную учетную запись Administrator, группу администраторов домена и доменную учетную запись Other1, которую вы создали для контрактника. Сразу же, как только эта политика вступит в силу, все неуказанные учетные записи будут из группы удалены, а все указанные, отсутствовавшие в ней на тот момент, добавлены.

Примечание.

Если вы не включите в эту группу ее первоначальных членов (Administrator и группу Domain Admins), то своими руками отберете у себя администраторские привилегии на локальных компьютерах.

На каком уровне применить эту политику? Первое, что приходит в голову, — на уровне домена, поскольку в наши намерения входит применить ее ко всем компьютерам сети. Но это решение неверное. Среди компьютеров домена есть контроллер домена. Его учетная запись, правда, принадлежит организационной единице Domain Controllers, но политика домена будет применена к нему в порядке наследования. А это значит, что группа Enterprise Admins перестанет быть членом группы локальных администраторов на нем, что может повлечь нарушение работы домена.

Значит, нужно создать объект групповой политики над контейнером Computers, объединяющим рядовые компьютеры, не контроллеры домена? Не получится, потому что объекты групповой политики можно применять только к домену и организационным единицам, а контейнер Computers таковым не является.

Решение есть: нужно создать организационную единицу и переместить в нее учетные записи рядовых компьютеров.

1. Запустите консоль **Active Directory — пользователи и компьютеры** от имени администратора.
2. Сразу же под уровнем домена (то есть на уровне ранее созданных подразделений) создайте новую организационную единицу с названием «Компьютеры».
3. Переместите в нее все учётные записи компьютеров из контейнера Computers.
4. Отобразите окно свойств новой организационной единицы и перейдите на вкладку **Групповые политики**.
5. Нажмите кнопку **Создать**. Появится новый объект групповой политики. Дайте ему имя «Local administrators membership » (членство в группе локальных администраторов).
6. В новом объекте групповой политики раскройте ветвь **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности.**

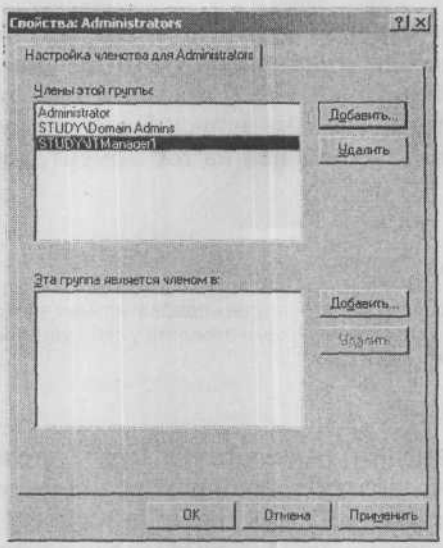


Рис. 17.5. *Группа с ограниченным доступом Administrators*

7. Щелкните правой кнопкой мыши по политике **Группы с ограниченным доступом** и из контекстного меню выберите команду **Добавить группу**.
8. В диалоговом окне **Добавить группу** введите (без опечаток) название Administrators и нажмите **OK**.
9. В диалоговом окне свойств группы, в верхней части, нажмите кнопку **Добавить** и введите регистрационное имя `Administrator`. Потом нажмите кнопку **Обзор** и выберите группу `STUDY\Domain Admins` и доменную учетную запись `STUDY\Other1`.

Активация политики в отношении компьютеров

Когда только что настроенная политика вступит в силу, на каждом компьютере домена под управлением Windows XP Professional или Windows 2000 в группе локальных администраторов появится еще один член — доменная учетная запись временного работника. Доменная группа администраторов останется без изменений. Но когда она вступит в силу?

- После перезагрузки компьютера. При каждой загрузке компьютер опрашивает контроллеры доменов о наличии объектов групповой политики, которые применимы к этому компьютеру, применяет их и только после этого выводит диалог регистрации пользователя.
- К уже работающим в домене компьютерам политики будут применены постепенно (через 90 минут плюс-минус случайная величина от 1 до

30 минут). Исключение составляют контроллеры домена, на которых новая политика вступает в силу через 5 минут.

- Когда на клиентском компьютере (под управлением Windows XP Professional или Windows Server 2003) будет запущена утилита командной строки GPUPDATE. В Windows 2000 вместо нее служит команда

```
secedit /refreshpolicy machine_policy /enforce
```

Как и для политик в отношении пользователей, интервал обновления можно сменить. Для этого служит политика **Интервал обновления групповой политики для компьютеров** в разделе **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика.** Установите там постоянную и случайную части нового интервала. Там же находится параметр **Отключить фоновое обновление групповой политики**. Чтобы ввести в силу эту политику, компьютер необходимо перезагрузить.

Группы с ограниченным доступом являются весьма мощным средством. Из примеров мы видим, что это средство можно использовать как «сторожевую собаку» членства в важных доменных группах (в таком случае необходимо создать объект над организационной единицей Domain Controllers). Если кто-то из администраторов добавит в группу `Domain Admins` постороннего, то применение этой политики позволит через пять минут лишить его незаслуженных привилегий.

В начале этого параграфа мы говорили о задаче, для которой нужно сделать администратором временного работника. За сроком его полномочий вам придется следить самим: либо изъяв его из группы с ограниченным доступом и активировав новую политику, либо ограничив срок действия его доменной учетной записи. Сама политика действует бессрочно.

17.4. Ограничьте пользователей в действиях, которые им для работы не нужны

Этот параграф тесно связан с первым параграфом настоящей главы, в котором мы тщательно скрывали от пользователей всё, что могло бы их отвлекать. Теперь мы дополним те ограничения новыми — разными для разных подразделений.

Больше всего ограничений наложим на работников склада. В их распоряжении должно быть только одно приложение — почтовый клиент. Мы закроем им доступ к Панели управления и ограничим возможности Проводника Windows.

Сотрудникам отдела маркетинга нужно менять язык и раскладку клавиатуры. Сначала вы полагали, что вы также запретите им доступ к окну Панель управления, но как же теперь? Решение может быть другим и, разумеется, оно существует.

Директора, разумеется, никаких ограничений не потерпят. Вам придется предоставить им полную волю и готовиться к ликвидации последствий их деятельности путем переустановки операционной системы на их компьютеры.

Итог по подразделениям:

- Store — добавить ограничения (Панель управления, Проводник Windows).
- Marketing — добавить ограничения (Панель управления).
- Managers — отменить назначенные ограничения.

17.4.1. Настройка ограничений для склада

Настройка ограничений в данном нашем случае будет строиться следующим образом:

1. Запустите консоль **Active Directory — пользователи и компьютеры** от имени администратора.
2. Отобразите свойства организационной единицы «Склад» и перейдите на вкладку **Групповые политики**.
3. Нажмите кнопку **Создать**. Появится новый объект групповой политики. Дайте ему имя «Store limitations» (ограничения пользователей со склада).
4. В новом объекте групповой политики раскройте ветвь **Конфигурация пользователя\ Административные шаблоны\Панель управления**. Включите политику **Запретить доступ к панели управления.**
5. Раскройте ветвь **Конфигурация пользователя\ Административные шаблоны\Компоненты Windows\Проводник** и включите следующие политики:
   - **Удалить команды «Подключение сетевого диска» и «Отключение сетевого диска».**
   - **Скрыть выбранные диски из окна «Мой компьютер».**
   - **Удалить вкладку «Безопасность»** (действует только для Windows XP Professional и Windows Server 2003).
   - **Скрыть значок «Соседние компьютеры» в папке «Сетевое окружение».**

17.4.2. Настройка ограничений для отдела маркетинга

Поскольку пользователи из маркетинга должны работать с иностранными языками и раскладками клавиатуры, им нужен, собственно, доступ к одному апплету Панели управления — **Язык и региональные стандарты.**

1. Запустите консоль **Active Directory — пользователи и компьютеры** от имени администратора.
2. Отобразите свойства организационной единицы «Маркетинг» и перейдите на вкладку **Групповые политики**.
3. Нажмите кнопку **Создать**. Появится новый объект групповой политики. Дайте ему имя «Marketing limitations».
4. В новом объекте групповой политики раскройте ветвь **Конфигурация пользователя\ Административные шаблоны\Панель управления**.
5. Включите политику **Отображать только указанные элементы панели управления.** Нажмите кнопку **Показать** и введите (без опечаток) название «Язык и региональные стандарты».

17.4.3. Отмена ограничений для руководства

Для отмены ограничений:

1. Запустите консоль **Active Directory — пользователи и компьютеры** от имени администратора.
2. Отобразите свойства организационной единицы «Дирекция» и перейдите на вкладку **Групповые политики**.
3. В нижней части вкладки установите флажок **Блокировать наследование политики** и нажмите **ОК**.

Тем самым вы отменили применение политик, действующих на вышерасположенные уровни иерархии активного каталога, к текущей организационной единице. Этот флажок прерывает наследование всех примененных выше политик, что нас не устраивает: мы хотели бы отменить для подразделения только действие объекта групповой политики «Сокрытие ненужных файлов», а действие Default Domain Policy сохранить.

Существует возможность принудительно применить групповую политику, настроенную для некоторого контейнера, ко всем контейнерам более низкого уровня, даже если у них заблокировано наследование политики. Воспользуемся ею для объекта Default Domain Policy:

4. В окне консоли **Active Directory — пользователи и компьютеры** отобразите свойства домена `study.local` и перейдите на вкладку **Групповые политики**.
5. Выберите объект Default Domain Policy. Нажмите кнопку **Параметры**. В появившемся диалоговом окне установите флажок **Не пере-**

крывать. После этого ни один нижестоящий контейнер не сможет переопределить (перекрыть) политики, примененные к родительскому контейнеру.

17.5. Обеспечьте безопасность хранения документов пользователей

В главе 13 мы разобрались с локальными и перемещаемыми профилями и выяснили, что оптимальным местом для хранения личных документов является папка «Мои документы», по умолчанию являющаяся частью профиля. У пользователей с локальными профилями при этом личные документы хранятся на той рабочей станции, за которой они работают, а у пользователей с перемещаемыми профилями — на сервере.

У обоих вариантов есть свои недостатки. В первом случае данные хранятся недостаточно надежно, так как жесткие диски пользовательских компьютеров обычно не архивируются. Во втором случае объём пользовательских данных, передаваясь по сети на компьютер, за которым пользователь раньше не работал, может существенно затормозить процесс регистрации.

Решением обеих проблем является переадресация папки «Мои документы» на сервер. Серверы регулярно архивируются, и данные пользователей таким образом сохраняются. При использовании перемещаемых профилей содержимое папки **документы** после переадресации перестаёт быть частью профиля, а вместо него в профиле сохраняется путь к переадресованной папке `\\сервер\папка`.

Создайте предварительно на сервере папку, которая станет родительской папкой для всех переадресованных личных папок, и откройте к ней сетевой доступ.

Для этого зарегистрируйтесь на PC001 и запустите консоль **Управление компьютером**.

1. Щелкните правой кнопкой мыши по значку **Управление компьютером** и из контекстного меню выберите команду **Подключиться к другому компьютеру**. Введите имя SRVR001 и нажмите OK.
2. Разверните контейнер **Служебные программы\Общие папки** и из контекстного меню выберите команду **Создать**. Укажите путь к папке C:\Home и дайте папке имя «Home». Нажмите **Далее**.
3. Установите флажок **Все пользователи имеют полный доступ**.

Поскольку мы собираемся переадресовывать папки «Мои документы» для всех пользователей, создадим для этой цели объект групповой политики на уровне домена:

1. Запустите консоль **Active Directory — пользователи и компьютеры** от имени администратора.
2. Отобразите свойства домена `study.local` и перейдите на вкладку **Групповые политики**.
3. Нажмите кнопку **Создать**. Появится новый объект групповой политики. Дайте ему имя «MyDocs redirection» (перенаправление папки «Мои документы»).
4. В новом объекте групповой политики выберите узел **Конфигурация пользователя\ Конфигурация Windows\Перенаправление папки**. Щелкните правой кнопкой мыши по папке «Мои документы» и из контекстного меню выберите команду **Свойства**.
5. На вкладке **Размещение** выберите в поле **Политика** значение **Простое — перенаправлять папки всех пользователей в одно место**.
6. В области **Размещение конечной папки** выберите **Создать папку для каждого пользователя на корневом пути**.
7. В поле **Корневой путь** введите путь `\\SRVR001\Home` и нажмите **ОК**. Для каждого отдельного пользователя в папке Home будет создана подпапка с его регистрационным именем.
8. Перейдите на вкладку **Параметры** и установите переключатели так, как показано на рис. 17.6.

Чтобы от имени рядового пользователя (например, `Shop1`) проверить путь к папке «Мои документы», нужно отобразить ее свойства. Но мы уже запретили это с помощью групповых политик (запретив показывать контекстное меню для элементов меню Пуск). Чтобы вытащить значок

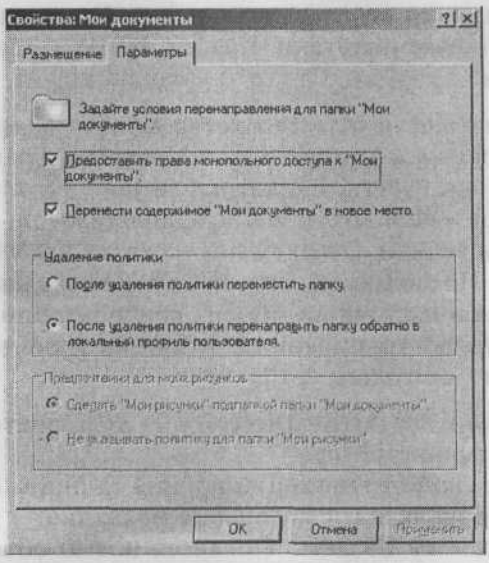


Рис. 17.6. *Параметры политики перенаправления папки*

папки «Мои документы» на рабочий стол (это не запрещено), выполните следующее:

1. Откройте окно свойств рабочего стола и перейдите на вкладку **Рабочий стол**.
2. Нажмите кнопку **Настройка рабочего стола** и в диалоговом окне **Элементы рабочего стола** установите флажок **Мои Документы**. После этого вы сможете отобразить свойства этой папки.

Значок перенаправленной папки в ОС Windows XP Professional и Windows Server 2003 отличается двумя синими стрелками. Это указание на то, что содержимое папки на рабочей станции синхронизируется с сервером каждый раз при подключении и отключении пользователя от сети. Возможность автономной работы особенно удобна для пользователей с ноутбуками.

В Windows 2000 режим автономной работы по умолчанию не включен. Настроить его можно через политики в ветви **Конфигурация пользователя\Административные шаблоны\Сеть\Автономные файлы.**

17.6. Дисковые квоты. Настройка дисковых квот

Полезно бывает ограничить дисковое пространство, которое пользователи имеют право занять своими файлами. Это можно сделать как в свойствах каждого раздела, если он отформатирован файловой системой NTFS, так и через групповые политики. Как вы думаете, какое решение будет более системным?

Нужные нам политики находятся в ветви **Конфигурации компьютера**, то есть будут применены к компьютеру независимо от того, какой пользователь на нем сейчас зарегистрирован. Главное — это сделать так, чтобы содержание папок «Мои документы», хранящихся на сервере SRVR001, не было слишком велико. Отведем под каждую 200 Мб и еще 10 Мб для прочих настроек. Поскольку мы ограничиваем место на сервере SRVR001, который является в настоящий момент контроллером домена, нам нужно определить объект групповой политики на уровне организационной единицы Domain Controllers.

1. Запустите консоль **Active Directory — пользователи и компьютеры** от имени администратора.
2. Отобразите свойства организационной единицы Domain Controllers и перейдите на вкладку **Групповые политики**.
3. Нажмите кнопку **Создать**. Появится новый объект групповой политики. Дайте ему имя «Disk quotas».

4. В новом объекте групповой политики выберите узел **Конфигурация компьютера\ Административные шаблоны\Система\Дисковые квоты**. Настройте политики следующим образом:
   - **Включить дисковые квоты**: Включено.
   - **Задать предел дисковой квоты**: Включено.
   - **Предел квоты по умолчанию и уровень предупреждения**: 210 Мб, 190 Мб.
   - **Вести журнал при превышении предела квоты**: Включено.
   - **Заносить событие превышения уровня предупреждения**: Включено.

Дисковые квоты будут применяться ко всем пользователям, кроме членов группы администраторов. А как иначе они смогли бы устанавливать на сервер громоздкие приложения?

17.7. Результирующая политика

Вы только что вернулись из отпуска и начисто забыли, кого ограничили, в чем и при помощи каких политик, а пользователи уже стоят в очереди с жалобами на недостаток прав. Точно выяснить, какой объект групповой политики за какие настройки отвечает, поможет оснастка **Результирующая политика,** присутствующая в Windows XP Professional.

1. Зарегистрируйтесь на PC001 под именем пользователя, который жалуется (пусть это будет Store1).
2. Выполните команду **Пуск → Выполнить** и введите команду **mmc**.
3. В пустую консоль MMC добавьте изолированную оснастку **Результирующая политика.** Запустится Мастер, в окнах которого согласитесь с параметрами по умолчанию, пять раз нажав **Далее**, и после завершения анализа компьютера нажмите **Готово**.
4. В добавленной оснастке разверните ветвь **Конфигурация пользователя\Административные шаблоны\Панель задач и меню «Пуск»**. В правой части окна отобразятся политики из разных объектов, которые вместе образуют конфигурацию для данного пользователя. В последнем столбце указано имя объекта групповой политики, которому принадлежит действующее значение политики.

Если вы сидите на своем рабочем месте, а жалуются с другого компьютера, то подходить к нему необязательно: достаточно в окнах Мастера результирующей политики указать имя другого компьютера и учетной записи пользователя.

Оснастку **Результирующая политика** можно запустить также, введя команду **rsop.msc**. По этой команде будет проанализирована конфигурация для локального компьютера и зарегистрированного сейчас пользователя.

Кстати, а почему у вас под именем администратора не запускается редактор реестра? Проанализируйте результирующую политику для себя, и вы обнаружите, что на вас влияют объекты Default Domain Policy, «Сокрытие ненужных файлов» и «Перенаправление папки». Ограничениями заведует второй из них.

1. Запустите консоль **Active Directory — пользователи и компьютеры**.
2. Отобразите свойства домена `study.local` и перейдите на вкладку **Групповые политики**.
3. Отобразите свойства объекта «Сокрытие ненужных файлов» и перейдите на вкладку **Безопасность**. Вы видите, что группа «Прошедшие проверку» («Authenticated Users») имеет разрешения на чтение и применение групповой политики. Это именно то разрешение, которое вас как администратора не устраивает: объект групповой политики применяется ко всем нижестоящим контейнерам только тогда, когда они имеют эти разрешения.
4. Выберите в списке субъектов доступа группу Domain Admins и запретите для нее применение групповой политики. Теперь ваша учетная запись не будет подлежать ограничениям.

Эта процедура называется фильтрацией объектов групповой политики.

17.8. Замыкание пользовательской политики

Если вы думаете, что хорошо поняли и усвоили материал настоящей главы, то этот параграф — специально для вас.

Вот ситуация: обычно пользователь, отходя от своего рабочего места ненадолго, не завершает сеанс, а просто блокирует компьютер нажатием комбинации клавиш Ctrl+Alt+Del. Снять блокировку может он сам, зная пароль, или администратор, но никто другой, поэтому на компьютерах, стоящих в общественных местах, блокировка нежелательна. А у нас есть компьютеры в торговом зале, на которых работают разные сотрудники отдела продаж — кто за каким придется — и поэтому практику блокировки на этих компьютерах следовало бы запретить.

Политика **Запретить блокировку компьютера** находится в контейнере **Конфигурация пользователя\Административные шаблоны\Система\Возможности Ctrl+Alt+Del.** Но проблема в том, что применить ее надо не к отдельным пользователям, а к отдельным компьютерам (пусть это будет компьютер PC001).

Способ решения этой проблемы называется замыканием пользовательской политики и состоит в том, что при регистрации на компьютере, для которого действует политика замыкания, объекты групповой политики компьютера определяют, какие из объектов групповой политики пользователя следует здесь применить.

1. Зарегистрируйтесь на PC001 и запустите консоль **Active Directory — пользователи и компьютеры**.
2. Создайте в организационной единице «Компьютеры» дочернюю организационную единицу «Торговый зал» и переместите в нее учетную запись PC001.
3. Отобразите свойства организационной единицы «Торговый зал», перейдите на вкладку **Групповые политики** и создайте новый объект с именем «No Lock» (запрет блокировки).
4. В новом объекте раскройте ветвь **Конфигурация пользователя\Административные шаблоны\Система\Возможности Ctrl+Alt+Del** и включите политику **Запретить блокировку компьютера.**
5. Выберите узел **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика.** Включите эту политику и из списка **Режим** выберите **Слияние**. Режим слияния требует, чтобы к пользователю были применены не только политики, настроенные для него, но и политики, настроенные для компьютера (режим замены — только политики компьютера).

17.9. Порядок применения групповых политик

Объекты групповой политики можно определять на разных уровнях иерархии активного каталога: на локальном компьютере, на уровне домена, организационной единицы и сети. С локальными политиками мы познакомились еще в среде рабочей группы. С политиками на уровне сайта (они задаются с помощью консоли **Active Directory — сайты и службы**)) вы будете сталкиваться не часто, поскольку они предназначены для крупных сетей.

Порядок применения политик нужно знать на случай, если значения одной и той же политики в разных объектах, последовательно примененных к учетной записи, конфликтуют между собой. Сначала применяются локальные политики, потом политики на уровне сайта, потом политики домена, потом политики организационных единиц сверху вниз. Приоритет имеют те политики, которые ближе к учетной записи. То есть если на уровне домена пользователю разрешено изменять рабочий стол, то это еще ничего не говорит о его правах: ему может быть запрещено на уровне подразделения.

Объекты одного уровня применяются снизу вверх, то есть приоритет имеют те объекты, которые расположены выше. Порядок объектов можно менять.

Применение объектов групповой политики можно изменить с помощью фильтров WMI, выбирающих из контейнеров только компьютеры с указанными свойствами. Например, вы можете применить некоторую политику только к тем компьютерам, у которых процессор быстрее, чем 733 МГц или установлен Service Pack 1. Примеры фильтров WMI:

- Компьютеры, на которых установлен модем:

```
Root\CimV2; Select * from Win32_POTSModem
```

- Компьютеры с указанной операционной системой:

```
Root\CimV2; Select * from Win32_OperatingSystem where
Caption = "Microsoft Windows XP Professional"
```

- Компьютеры, где хотя бы на одном разделе NTFS свободно больше 10 Мб:

```
Root\cimv2; SELECT * FROM Win32_LogicalDisk
WHERE (Name = „C:" OR Name = „D:" OR
Name = „E:") AND DriveType = 3 AND FreeSpace > 10485760
AND FileSystem = „NTFS"
```

- Компьютеры, где установлено приложение с указанным идентификатором:

```
Root\cimv2; SELECT * FROM Win32_Product
WHERE IdentifyingNumber =
„{5E076CF2-EFED-43A2-A623-13E0D62EC7E0}"
```

17

Для администрирования объектов групповой политики служит утилита GPMC (Group Policy Management Console). Кроме гораздо большего удобства работы, она позволяет архивировать объекты, переносить их в другой домен и управлять ими из командной строки. Эта утилита не входит в стандартную поставку Windows Server 2003.

В свойствах объектов групповой политики на вкладке **Общие** есть флажки **Запретить настройку конфигурации компьютера** и **Запретить настройку конфигурации пользователя.** Если объект содержит только политики одного типа, то запрет применения политик второго типа ускорит процесс загрузки компьютера или регистрации пользователя.

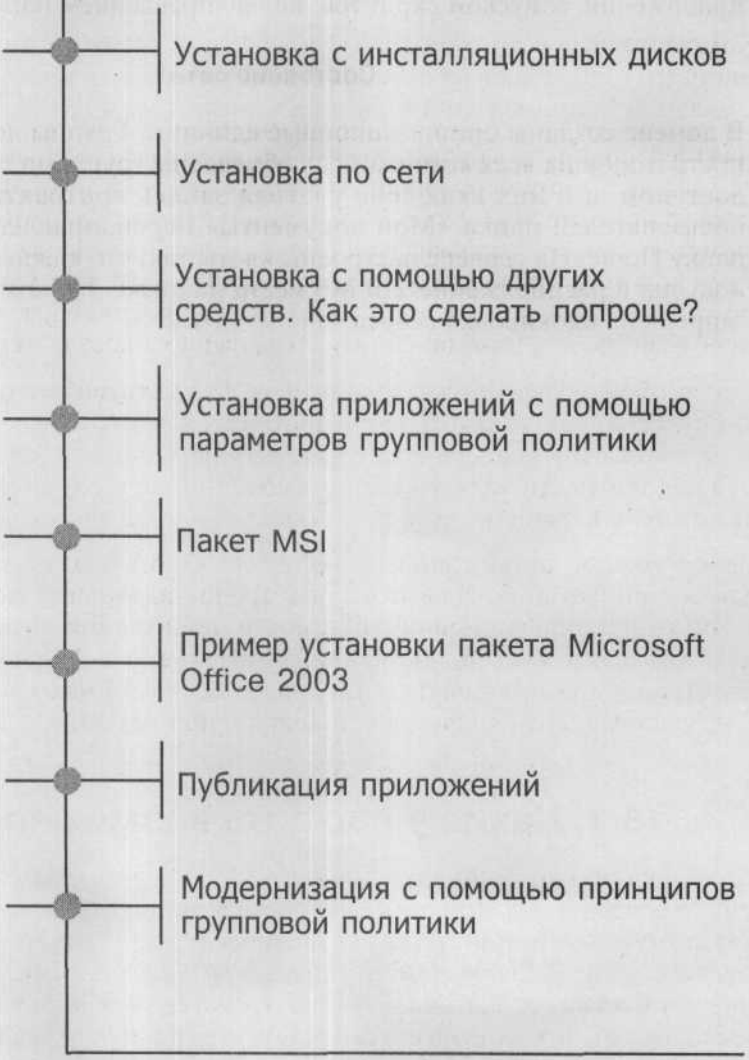
17.10. Итоги

Инструмент **Групповые политики** — это одно из мощнейших средств системы Windows Server 2003, позволяющее просто, быстро и единообразно администрировать пользовательские компьютеры. Система Windows XP Professional содержит более 700 политик, управляющих видом и поведением пользовательских компьютеров, их безопасностью, установкой приложений, запуском скриптов, перенаправлением папок и т.п.

Состояние сети

В домене созданы организационные единицы. Группы локальных администраторов на всех компьютерах объявлены группами с ограниченным доступом, и в них включена учетная запись контрактника. Для всех пользователей папка «Мои документы» перенаправлена на сервер, в папку Home. На сервере настроены квоты так, что каждый пользователь получил в распоряжение 210 Мб места на диске. На компьютере PC001 запрещена блокировка сеанса.

Глава 18 Устанавливаем приложения



Компьютерные сети существуют не для того, чтобы в них работали администраторы, а для того, чтобы упростить работу пользователей с документами и приложениями, которые нужны им для работы.

Для всех сегодня сеть представляется как само собой разумеющееся. Никого не удивляет, к примеру, что к Интернету они подключаются сразу после запуска приложения Internet Explorer и им не нужен для этого модем; если им нужен какой-то важный файл, они откроют его из папки на сервере, а не будут ходить за тридевять земель с дискетой; и если они хотят распечатать фотографию своего домашнего любимца, они просто пошлют её на принтер, даже если он не подсоединён непосредственно к компьютеру.

Само собой, кто-то может напомнить, что сеть может принести и неприятности, как то быстрое распространение вирусов, нежелательные электронные письма (спам) и тому подобное. Он будет, несомненно, прав. Эти неприятности являются чем-то вроде «естественной болезни» сетей, от которой, к счастью, есть лекарства.

Целью каждой организации является то, чтобы пользователи работали для её процветания. Для этого она предоставляет всё необходимое — компьютер с операционной системой и приложениями. Компьютер мы пользователям уже предоставили, к тому же ещё в предыдущей главе мы ограничили пользователей в действиях, не нужных им для работы. Следующим шагом является установка приложений.

18.1. Какие у нас есть возможности?

Установка приложений для администратора всегда кошмар. Речь идёт о чём-то более глобальном, нежели просто администрирование операционной системы. Администратор уже наперёд знает, что его ждёт работа с подготовкой установки, само её проведение и решение проблем. В небольших организациях опасения администраторов, в общем-то, обоснованы, поскольку от них автоматически ждут, что они будут для пользователей чем-то вроде службы поддержки.

Руководство компании предполагает, что администраторы существуют для того, чтобы решать любые проблемы, касающиеся оборудования,

системы, приложений и многого другого. Автоматически администратор становится экспертом в области любого приложения, использующегося в сети. Это, однако, является большой ошибкой. Такого рода администратор, по сути дела, — раб, который проводит за работой все время только для того, чтобы хотя бы удержать систему на плаву.

Поскольку работы много, он ничего не делает как следует и до конца, у него нет времени ничему научиться и вследствие этого появляются новые ошибки, которые опять надо исправлять. Круг замкнулся...

Со стороны администратора должна быть осуществлена установка приложений в пространстве сети. Остальное — поддержка приложений, при случае, их администрирование — должно являться обязанностью отдела технической поддержки, при возможности — поставщика программного обеспечения.

Вот мы и подошли в нашей к сети к установке нескольких приложений. Давайте же посмотрим, какие у нас есть варианты.

18.2. Установка с инсталляционных дисков

Речь идёт о самом простом способе установки приложения. Администратор возьмет диск, подойдет к компьютеру, выгонит из-за него пользователя, войдет в систему под учетной записью администратора и проведет установку. И так с каждым компьютером.

Это всё прекрасно работает до тех пор, пока не появляются проблемы. Какие?

Запуск приложения от имени другого пользователя

Типичная проблема, возникающая у приложений Microsoft Office 2003. При входе нового пользователя и запуска приложения из этого пакета происходит настройка приложений для данного пользователя, для чего требуется установочный диск. Неприятная, и, как мне кажется, в данном случае безвыходная ситуация.

Пользователь по ошибке удалил какой-то из файлов приложения

Хотя этот вариант благодаря разрешениям NTFS в системе Windows XP Professional почти полностью отпадает, он может о себе напомнить. Некоторым приложениям может потребоваться изменение прав доступа пользователя к папке, в которой установлено приложение, для изменения содержимого файлов приложением в процессе работы, и пользователь случайно может удалить важные файлы. После этого остаётся лишь взять компакт-диск, сесть за компьютер и повторить установку.

Пользователь хочет добавить компоненты приложения

Хотя среда установленных приложений однородна, могут появиться пользователи (и даже целые отделы), которые потребуют установки дополнительных возможностей приложения. Следующий шаг — такой же, как при первоначальной установке приложения. Самое существенное — это то, что к компьютерам должны подходить вы, т.к. требуется опять таки учетная запись администратора.

В компьютере нет привода CD-ROM

Весьма распространённое явление (в сегодняшних сетях). Приложение вы купили, диск у вас есть, вы готовы, но установку не выполнить. В этом случае ничего более не остаётся, как использовать другой метод установки.

18.3. Установка по сети

Данный способ установки отличается от предыдущего только тем, что установочным диском служит сеть. Принцип прост. На сервере (которым в данном случае является обычный файловый сервер) создается папка с установочными файлами приложения. С пользовательского компьютера вы впоследствии как администратор подключаетесь к папке и проводите установку приложения.

Этот способ установки имеет некоторую выгоду. Вы не должны будете носить с собой установочные диски и можете установить приложение на компьютер, который не располагает приводом CD-ROM, если только он имеет действующее подключение к сети.

Одновременно с этим данный способ установки может устранить неполадки, связанные с приложениями пакета Office 2000/2003 (или им подобными) при входе другого пользователя. Компьютер уже не будет требовать установочный компакт-диск: имея доступ к установочным файлам, он доустановит нужные данные автоматически.

18.4. Установка с помощью других средств. Как это сделать попроще?

Между администраторами сети Microsoft хорошо известно средство Systems Management Server 2.0. Речь идёт об очень хорошем средстве, которое может делать кучу разных вещей. Установка приложений — одна из них.

Его плюсы (в области установки приложений) включают возможность установки на компьютеры пользователей практически любого приложения. Минусом является необходимость покупки этого продукта, установки сервера и клиентской части на все компьютеры пользователей и, разумеется, умение всё это благополучно администрировать. Иными словами — нужно иметь в распоряжении ещё одного администратора, который и будет заботиться об управлении этой частью рабочего пространства. О расходах, которые потребуются на такого рода автоматизацию, речь не идёт.

Следующим средством для установки приложений является часть параметров групповой политики домена Active Directory под названием Установка программ. Ей мы посвятим разделы в следующих параграфов.

Я хочу кое-что предложить. А именно — как с помощью стандартных средств домена Active Directory подготовить автоматическую установку, которая позволит вам сделать для себя процес установки менее энергозатратным, в то время как вы будете изображать перед руководством, что работы у вас — выше крыши.

В домене Active Directory есть средства, которые вы можете использовать для автоматической установки приложений на компьютеры пользователей. Они являются частью групповой политики, так что правильным размещением ее объектов вы можете определить, какой пользователь будет иметь то или иное программное обеспечение.

18.5. Установка приложений с помощью параметров групповой политики

В предыдущей главе мы изучали параметры и объекты групповой политики. Была изложена вся необходимая информация, описано их применение, и также мы рассмотрели некоторые конкретные параметры. Хотя этого всего вполне достаточно, мы совсем не коснулись одной из возможностей групповой политики — Установки программного обеспечения.

18.5.1. Конфигурация компьютера или конфигурация пользователя?

Часть параметров групповой политики касается установки программного обеспечения и находится в обоих разделах объекта — **Конфигурация Компьютера** и **Конфигурация пользователя**. Нужно знать, какие между ними есть различия и что нам необходимо.

Конфигурация компьютера

Все параметры, сконфигурированные в этой ветви объекта групповой политики, всегда применяются только к учётным записям компьютера. Это нам хорошо знакомо. Если вы определите установку программного обеспечения в этой части, она будет касаться только компьютеров независимо от того, какой именно пользователь войдёт в систему.

Приложения, устанавливаемые с помощью установок в части **Конфигурация компьютера**, на первый взгляд, со стороны пользователя кажутся статичными, то есть остаются всегда в данном компьютере и доступны каждому пользователю, вошедшему в систему.

Конфигурация пользователя

Параметры в этой части объекта касаются только учётных записей пользователя. Предположим, что пользователям в отделе Склад (Store) вы предоставите только приложение Outlook (почтового клиента), а пользователям отдела маркетинга (Marketing) установите весь пакет Microsoft Office.

На любом компьютере, где зарегистрируется сотрудник отдела маркетинга, у него будут в распоряжении все приложения пакета Office. Если на этом же компьютере зарегистрируется работник склада (Store), он получит доступ только к приложению Microsoft Outlook.

Приложения, установленные при помощи настроек в ветви **Конфигурация пользователя**, «путешествуют» таким образом вместе с пользователем.

18.5.2. Примеры использования разных видов установок

Разницу между конфигурацией установки приложений посредством ветвей **Конфигурация компьютера** и **Конфигурация пользователя** мы покажем на примере установки пакета обновления Service Pack. С точки зрения администратора, обновление Service Pack операционной системы является обычным приложением, только очень важным.

Если вы определяете установку обновления Service Pack в разделе **Конфигурация компьютера**, вы обеспечиваете её установку на все компьютеры, связанные с объектом групповой политики, который вы для этих целей создали. Service Pack таким образом установится на компьютеры и будет в системе независимо от входящего пользователя.

Если вы эту установку определили в части Конфигурация пользователя объекта, который потом вы примените, например, на подразделение

Marketing, пакет Service Pack установится только на те компьютеры, на которых зарегистрированы пользователи из этого отдела. После их выхода их системы обновление будет удалено.

Со стороны администратора группы более разумным был бы первый вариант, то есть установка, определённая в части **Конфигурация компьютеров**.

Другим примером может послужить специальное антивирусное приложение, которое вы можете использовать только в единственном экземпляре. Как администратор вы решаете проблемы прямо у пользователей и в некоторых ситуациях вам нужно провести анализ компьютера на вирусы. Поскольку для этого антивирусных программ компьютеров пользователей недостаточно, вам нужно будет воспользоваться своей антивирусной программой.

Но вы не знаете наперёд, на каких компьютерах вам нужно будет её использовать. Установку этой антивирусной программы вы определите в объекте групповой политики, которая будет применяться только для учетной записи администраторов.

Если вы впоследствии войдёте в любую систему как администратор, у вас это приложение уже будет установлено.

18.5.3. Добавление или публикация приложения?

Мы стоим перед двумя понятиями, которые для использования параметров групповой политики в отношении установки программного обеспечения необходимо усвоить. Речь идёт о способе установки приложения и о том, как о нём узнают пользователи.

Добавление приложения

Добавление приложения — одна из возможностей установки, которую необходимо определить при подготовке инсталляционного пакета. Если вы добавите приложение, произойдёт следующее:

- После входа пользователя в меню **Пуск** появится ярлык этого приложения.
- Пользователь может запустить приложение щелчком по этому ярлыку или же запустив сам исполняемый файл.

Добавление приложения используется в случае, когда пользователи действительно нуждаются в этом приложении, и им нужно иметь их ярлык в меню **Пуск**.

Публикация приложения

С публикацией приложения дело обстоит иначе. После публикации приложения произойдёт следующее:

- Пользователь после входа в систему не найдёт ярлыка приложения в меню **Пуск**.
- Пользователь может запустить приложение через его установочный файл или апплет **Установка и удаление программ.**

Публикация приложения используется в случае, если у вас для пользователей приготовлены приложения, но вы не хотите их добавлять в меню **Пуск** и отводить под них место на диске.

Сочетания вида установки и раздела групповых политик *Таблица 18.1*

	Конфигурация компьютера	Конфигурация пользователя
Добавление приложения	Да	Да
Публикация приложения	Нет	Да

18.5.4. Немедленная или отложенная установка?

Параметры групповой политики из раздела **Конфигурация пользователя** применяются сразу после входа пользователя в систему и затем регулярно обновляются. Теперь представьте себе состояние, когда с помощью групповой политики мы определим установку набора офисных приложений на 100 компьютеров.

И если однажды утром так все сложится, что в систему войдут сразу 100 пользователей, что произойдёт? Установочный сервер не справится с нагрузкой и «зависнет»? Это зависит от того, каким образом вы сконфигурируете установку приложений.

У вас есть два варианта на выбор:

- **Отложенная установка.** В этом случае происходит установка данного приложения в момент, когда её запустит пользователь. При применении политики во время входа пользователя в систему произойдёт объявление приложения, созданное в форме ярлыка в меню **Пуск**. Вероятность, что всем 100 пользователям сразу потребуется одно и то же приложение, настолько мала, что перегрузка компьютера, откуда проводится установка, не предполагается.
- **Немедленная установка.** В этом случае происходит установка данного приложения сразу во время входа в систему пользователя. Например, владелец переносного компьютера вне сети смог бы только руками развести, почему это у него в меню **Пуск** есть приложение, которого на самом деле в компьютере нет. Поэтому данный тип установки

используется в основном у переносных компьютеров. Пользователи, однако, должны в этом случае рассчитывать на то, что процесс их входа в систему немного затянется на период установки всех приложений, которые вы определили в объекте групповой политики.

Примечание.

В домене Active Directory с системой Windows server 2003 немедленную установку можно использовать только при добавлении инсталляционного пакета.

18.5.5. Все приложения или только некоторые?

С помощью параметров групповой политики в доменах Active Directory можно устанавливать только инсталляционные пакеты MSI, то есть приложения, которые созданы для установочных служб системы Windows. Речь идёт о новой службе, которая есть в нашем распоряжении с момента появления системы Windows 2000.

Это, без сомнения, переломный момент в использовании параметров для установки программного обеспечения. Не все приложения добавляются в форме этого пакета. Если вы хотите удалённо установить приложение, вы должны решить, будет ли у вас инсталляционный пакет MSI и вы сможете использовать объект групповой политики или у вас будет только установочная программа в виде файла setup.exe и вы должны будете использовать Systems Management Server.

Возможность установки программного обеспечения с помощью групповых политик пришла на рынок вместе с системой Windows 2000 в конце 1999 года. Тогда был просто праздник встретить пакет MSI для необходимого приложения. Сегодня, спустя более чем 5 лет, ситуация кардинально изменилась.

18.6. Пакет MSI

Что же такое пакет MSI? Как выглядит его структура? Вспомните, мы уже встречались с ним при установке пакета администрирования домена на компьютер PC001 и модуля многоязыковой поддержки интерфейса.

Установка программ происходит посредством запуска `setup.exe`, а всё остальное устроит установочная программа. Что произойдёт в системе? Во время установки создаются новые папки, в которые разархивируются файлы, часть файлов может быть добавлена в системные папки, создаются новые записи в реестре и у пользователей появятся ярлыки в меню Пуск.

Такую установку вы могли провести и вручную. Если бы вы достали утилиты для разархивирования и информацию о том, какие папки и ключи в реестре и где нужно создать и что куда скопировать, вы смогли бы сделать все самостоятельно. Результат получился бы тот же, но, в сравнении с установочной программой, более медленно.

Файл MSI является объектом, содержащим именно такую информацию: что и где создать, какие папки и ключи в реестре, какие файлы куда скопировать и т.п. Кроме файла MSI, существуют и другие файлы, являющиеся частью установки. Если приложение невелико, установочные файлы являются частью файла MSI. Он содержит в себе две части — базу данных и файлы (вспомните файл `adminpak.msi` или `twclient32.msi`, оба в стиле «все в одном»).

18.7. Пример установки пакета Microsoft Office 2003

Несмотря на то, что я встречал разных администраторов, которые знали о возможности установки приложений с помощью объектов групповой политики, у них у всех преобладало мнение, что такая установка «нормально не функционирует» и было бы проще и лучше установить всё вручную.

Часто в таких случаях речь шла об установке приложений пакета Microsoft Office, что огорчает вдвойне. Во-первых, Office выпускается в виде пакета MSI, начиная с версии 2000, а во-вторых, — речь идёт о продукте компании Microsoft. А что ещё может функционировать нормально вместе, как не продукты Microsoft?

Конечно, временами и в компании Microsoft принимаются решения, которые не столь хороши, как их рекламируют. Такие оплошности быстро исправляются и затем нормально функционируют.

18.7.1. Стратегия установки приложений пакета Office 2003

Все пользователи компании Study должны по идее иметь приложение Outlook — органайзер для работы с контактами, заданиями и электронной почтой.

Пользователи в отделе продаж и маркетинга нуждаются в приложениях Word и Excel. Они работают с этими приложениями ежедневно, так что установим им эти приложения так, чтобы они отобразились в меню **Пуск**.

Пользователи на складе хоть и не являются типичными представителями классических офисных работников, но иногда им необходим редактор Word. И в этом случае мы пойдём пользователям навстречу и сконфигурируем приложение так, чтобы оно было подготовлено к установке, но не было отображено в меню **Пуск**.

Директорам всегда необходим полный набор приложений, даже если они и не знают, для чего те нужны. В своих компьютерах (и в каждом компьютере, в систему которого они войдут) эти приложения должны просто быть. Мы пойдём им навстречу и приложение Outlook обогатим полным комплектом пакета Office — Word, Excel и Access. Они будут единственными, кто будет располагать средством Microsoft Access.

Конфигурацию всех приложений мы проведём так, что приложения будут устанавливаться по требованию (отложенная установка). Пользователи будут видеть значок программы в меню **Пуск**, но до первой установки дело дойдёт только в случае необходимости использования.

В итоге — нам потребуется 4 типа инсталляционных пакетов (пакет для Продаж и Маркетинга, для Склада, для Руководства и для остальных). Значит ли это, что у нас на сервере будет несколько видов установочных файлов?

Необязательно. Можно использовать трансформирующий файл MST. А комплекс MSI+MST=установочный комплекс (вспомните файл ответа и единственный файл базы данных UDF — это было нечто подобное).

Мы, таким образом, будем использовать единый инсталляционный пакет MSI, но в каждом объекте используем его модификацию MST.

18.7.2. Подготовка к установке пакета Office 2003. Установка Office 2003 Resource Kit

Для успешной установки нам понадобится следующее:

- **Установочный диск пакета Office 2003.** Внимание! Диск должен быть из мультилицензионной программы. Другие версии для этого типа установки использовать нельзя.
- **Средства администрирования пакета Office 2003 Resource Kit.** Эта функция необходима, и я лично считаю, что все, кто утверждает, что установка пакета Office с помощью параметров групповой политики невозможна, это средство вообще ни разу не использовали. Именно с его помощью мы будем способны создать трансформирующие файлы MST.

Чтобы не перегружать сервер (это было бы непрактично), мы проведём установку необходимых средств и все приготовления на клиентском компьютере PC001.

Утилиту **Office 2003 Resource Kit** можно скачать как файл `ork.exe` с веб-страницы компании Microsoft.

1. Войдите в компьютер PC001 как администратор.
2. Запустите файл ork.exe. Утилита **Office 2003 Resource Kit** (ORK) есть только на английском языке.
3. Согласитесь с условиями лицензионного соглашения и нажмите **Next**.
4. В диалоговом окне выбора типа установки оставьте параметры по умолчанию и нажмите **Next**.
5. В диалоговом окне **Begin installation** нажмите кнопку **Install**. Произойдёт установка утилиты.

18.7.3. Администраторская установка пакета Office 2003

Установка приложений пакета Office 2003 должна быть в компьютерах пользователей быстрой и автоматической. Как администратор, вы не должны допускать, чтобы пользователи имели какое-то отношение к установке. Одно из допустимых вмешательств пользователя в конце установки — ввод имени, фамилии и инициалов.

По этим причинам нельзя просто скопировать содержимое установочного компакт-диска в общую папку на сервере, откуда будет происходить установка. Нужно провести так называемую администраторскую установку, при которой вы зададите все необходимые параметры, подходящие всем пользователям.

Установка, однако, должна быть помещена в общую папку, к которой пользователи имеют право доступа хотя бы на чтение. Но об этом — в заключение данного раздела..

Администраторская установка производится непосредственно на сервере SRVR001 под именем администратора.

1. На диске D: создайте папку «InstallApp» и в ней подпапку «Office 2003».
2. Вставьте в привод CD-ROM установочный диск пакета Microsoft Office 2003 Professional.
3. Выполните команду **Пуск → Выполнить** и введите путь к файлу `setup.exe` и дополнительный ключ `/a` (рис. 18.1). Продолжайте нажатием кнопки **OK**.

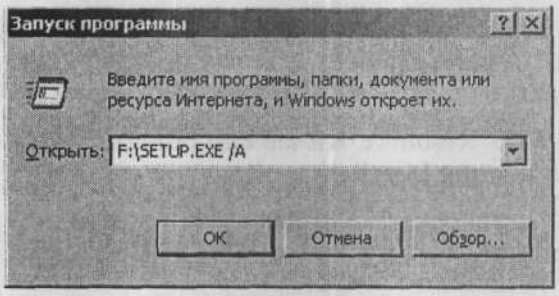


Рис. 18.1

4. Запустится установка приложений пакета Office. В следующем диалоговом окне задайте название компании, путь установки (D:\InstallApp\Office 2003) и код Product Key. Информацию, которую вы введёте в этом диалоговом окне, вы вводите вместо пользователей. Они таким образом при установке не должны будут ничего вводить, и установка произойдёт автоматически.
6. В следующем диалоговом окне прочтите лицензионное соглашение, согласитесь с ним и нажмите **Установить**.

Сейчас произойдёт установка продукта. Поскольку речь у нас идёт об администраторской установке, приложения не будут, как обычно, установлены на сервер и их невозможно будет запустить. Они будут просто подготовлены для установки на компьютеры пользователей.

18.7.4. Открытие доступа к папке InstallApp

1. Откройте окно свойств папки `InstallApp` и перейдите на вкладку **Доступ.** Откройте к ней сетевой доступ с сетевым именем `InstallApp`.
2. Группе Administrators дайте разрешение на **Полный доступ**, а группе Authenticated Users — на **Чтение**.

18.7.5. Трансформирующие файлы MST

Приготовленная установка приложений пакета Office теперь доступна пользователям. Перед тем как мы начнём создавать объекты групповой политики с параметрами установки, сначала необходимо подготовить трансформирующие файлы для отдельных типов установки. Для этого мы используем средство Custom Installation Wizard, которое мы уже установили как часть комплекса средств Office XP Resource Kit.

Создание трансформирующего файла для установки приложения Outlook

Для создания трансформирующего файла для установки Outlook:

1. Зарегистрируйтесь на PC001 как администратор.
2. Запустите **Custom Installation Wizard**. Начните работу нажатием кнопки **Next**.
3. В диалоговом окне **Open the MSI file** нажмите кнопку **Browse** и в сети на сервере SRVR001 в общей папке InstallApp найдите подходящий файл MSI (рис.18.2). Потом продолжайте нажатием кнопки **Next.**
4. В диалоговом окне **Open the MST file** оставьте выбранным поле **Create a new MST file** и потом нажмите кнопку **Next.**
   Другая возможность — **Open an existing MST file** — предназначена для исправления существующего файла MST. Нам она может потребоваться только в будущем при необходимых изменениях файлов MST.
5. В диалоговом окне **Select the File to Save** задайте имя и путь размещения файла MST. Исходным размещением будет та же самая папка, в которой находится файл MSI, тем не менее зависит от вас, какое размещение вы выберете. Файлу MST дайте название Outlook.MST и нажмите Next.

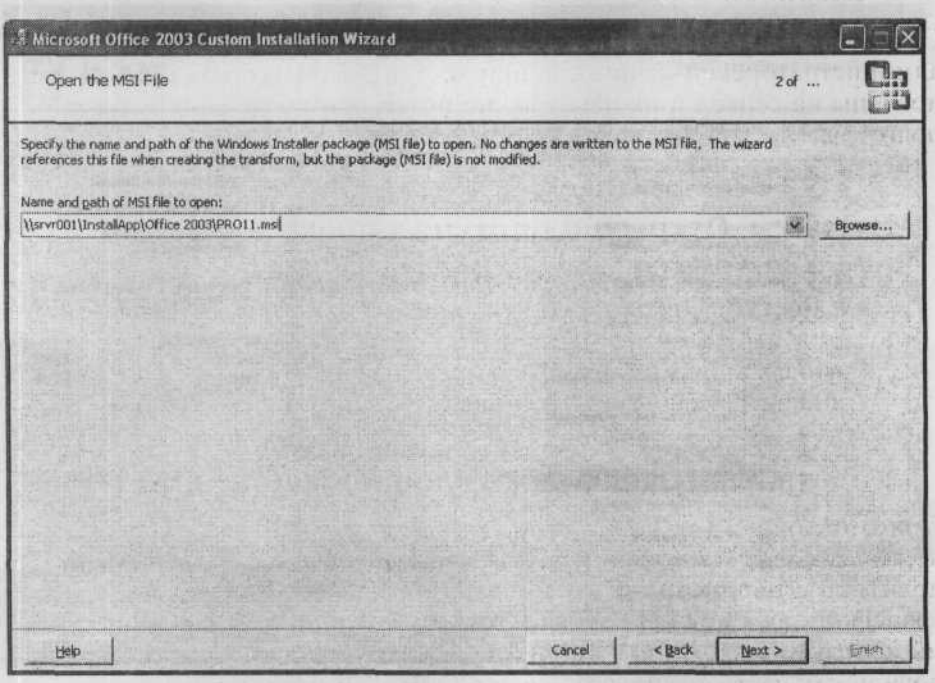


Рис. 18.2. *Путь к файлу MSI*

6. В диалоговом окне **Specify Default Path and Organization** (Укажите исходный путь и организацию) оставьте исходные установки. Значение <Default> в поле организации свидетельствует, что используется название, введённое при администраторской установке (Study). Нажмите **Next**.
7. В диалоговом окне **Remove Previous versions** (Удалить предыдущие версии) оставьте выбранными поля **Default Setup behavior** (Исходное поведение программы установки) и нажмите кнопку **Next**.
8. На вкладке **Set feature Installation States** (Выбор состояния установки) сконфигурируйте только установку приложения Outlook (Запустить всё с этого компьютера) и дополнения Помощник Office (он называется Office Assistant), который вы найдёте в части **Office Shared Features** (рис. 18.3). Нажмите **Next**.

Примечание.

Самым быстрым способом будет запретить установку на высшем уровне (всех компонент) и потом разрешить установку только нужных (Запустить с этого компьютера).

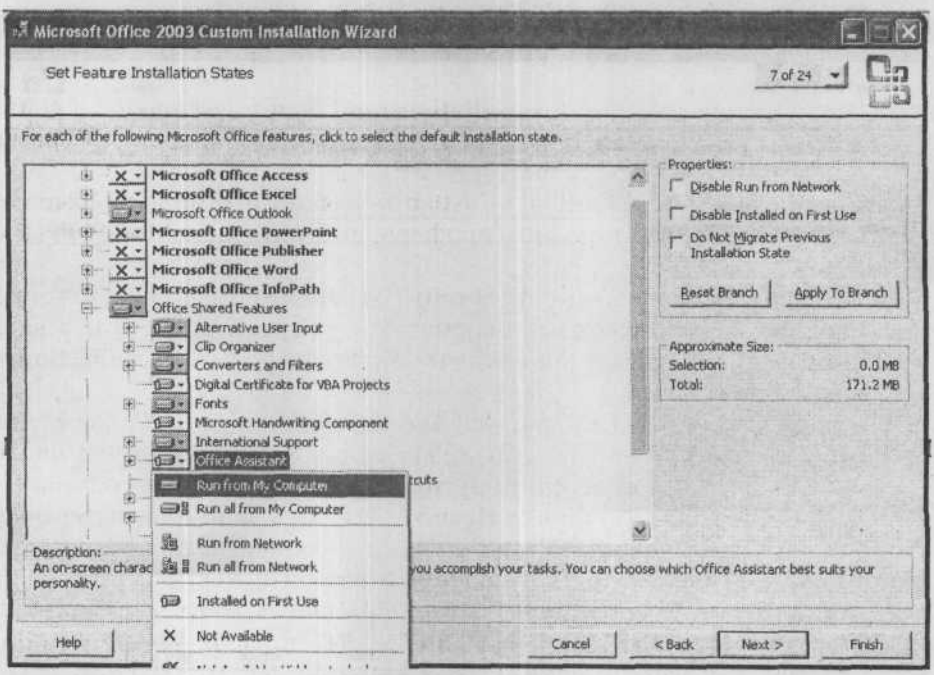


Рис. 18.3. *Конфигурация установки приложения Outlook*

9. В диалоговом окне **Customize Default Application Settings** (Задать исходные параметры приложения) оставьте выбранными поля **Do not customize** и **Migrate use settings** и нажмите **Next**.
10. В диалоговом окне **Change Office User Settings** откройте в левом подокне команду **Microsoft Outlook** и просмотрите возможные параметры. Никаких параметров не выбирайте (мы осуществим это позднее). Нажмите **Next**.
11. В диалоговом окне **Add/Remove files** (Добавить или Удалить файлы) нажмите **Next**. Здесь можно добавить к установке приложения любой файл, нам это не нужно.
12. В диалоговом окне **Add/Remove Registry Entries** (Добавить или Удалить записи реестра) нажмите кнопку **Next**. Не нужно добавлять или удалять никаких записей.
13. В диалоговом окне **Add, Modify, or Remove Shortcuts** (Добавить или Удалить ярлыки) исправьте на вкладке **Installed** список файлов так, как показано на рис.18.4, и нажмите **Next**.
14. В диалоговом окне **Identify Additional Servers** (Определить дополнительные серверы) не меняйте ничего и нажмите **Next**. Здесь добавляются дополнительные серверы, на которых находятся образы установки, они используются в случае недоступности исходного сервера.
15. В диалоговом окне **Specify Office Security Settings** (Задать параметры безопасности пакета Office) оставьте исходные параметры и нажмите **Next**.
16. В диалоговом окне **Add Installations and Run Programs** (Добавить установку дальнейших программ) не добавляйте никаких программ и нажмите **Next**.
17. В диалоговом окне **Outlook: Customize Default Profile** (Приложение Outlook: Изменить исходный профиль) выберите поле **Modify Profile** и нажмите **Next**.
18. В диалоговом окне **Outlook: Specify Exchange Settings** (Приложение Outlook: задать исходные параметры сервера Exchange) оставьте выбранными поля **Do not configure an Exchange server connection** и потом нажмите кнопку **Next**.
19. В диалоговом окне **Outlook: Add Accounts** (Приложение Outlook: Добавить учётные записи) оставьте выбранным поле **Do not customize Outlook profile and account information** и нажмите кнопку **Next**.
20. Диалоговое окно **Outlook: Remove Accounts and Export Settings** (приложение Outlook: Удалить учётные записи и экспортировать параметры) оставьте без изменений и нажмите **Next**.
21. В диалоговом окне **Outlook: Customize Default Settings** (Приложение Outlook: Исправить исходные параметры) оставьте установленные параметры и нажмите **Next**.

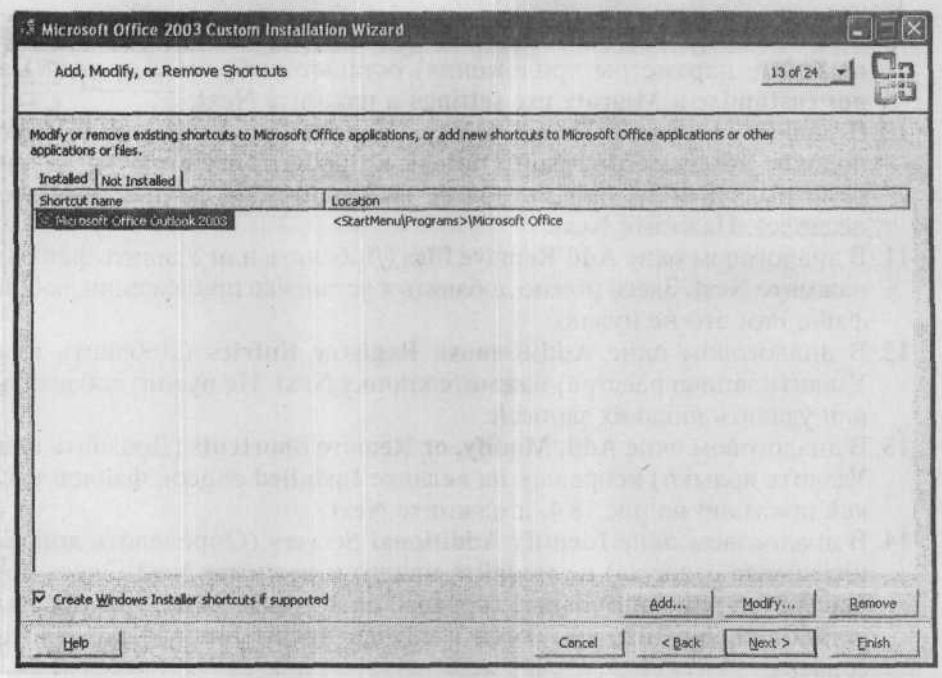


Рис. 18.4. *Исправление ярлыков в главном меню*

22. В диалоговом окне **Specify Send/Receive Group Settings** (Задание групповых установок) оставьте исходные параметры и нажмите **Next**.
23. В диалоговом окне **Modify Setup Properties** (Изменить свойства программы) оставьте исходные параметры и нажмите **Next**.
24. В диалоговом окне **Save Changes** (Сохранить изменения) нажмите **Finish**. Произойдёт сохранение конечного файла MST.

Информация, которая отобразится в диалоговом окне Custom Installation Wizard, нам не нужна (она нужна в случае установки вручную). Нажмите **Exit**.

Создание трансформирующего файла для установки приложений Outlook, Word и Excel

Повторяйте предыдущие действия со следующими изменениями:

- в пункте 5 задайте название файла **OutlookWordExcel.MST;**
- в пункте 8 обозначьте установку приложений **Microsoft Office Outlook,** (Запустить всё с этого компьютера) и в части **Office Shared**

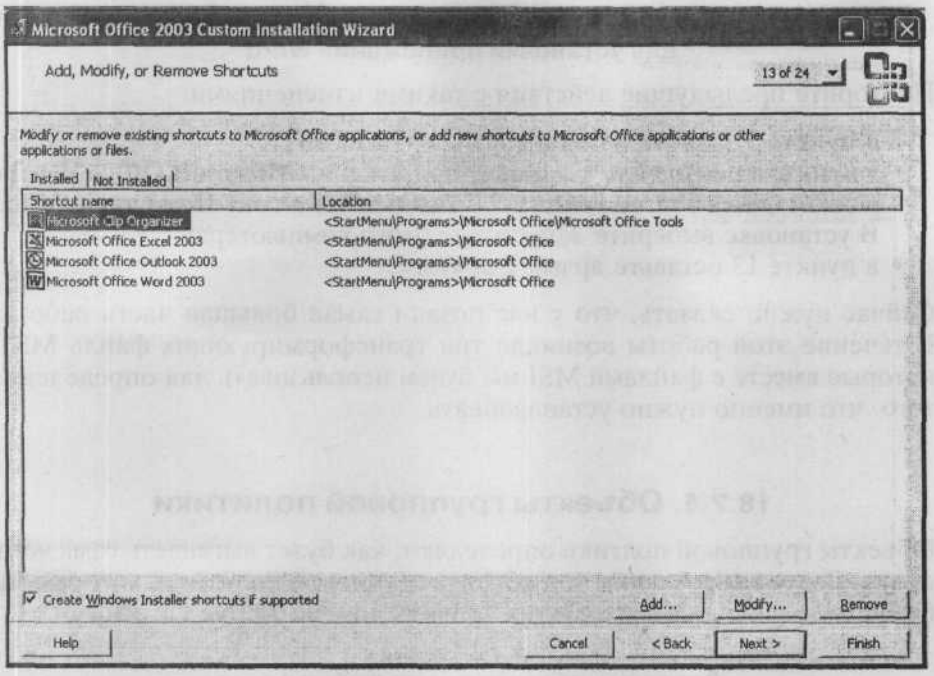


Рис. 18.5. *Исправление ярлыков меню Пуск*

Features обозначьте установку **Галерея клипарт и Помощник Office**. Для надежности проверьте, что произойдёт установка всех частей приложений Outlook, Word и Excel.

- В пункте 13 проведите конфигурацию согласно рис. 18.5.

Создание трансформирующего файла для установки приложений Outlook, Word, Excel и Access

Повторите предыдущие действия со следующими изменениями:

- в пункте 5 задайте название файла **AccessOutlookWordExcel.MST**;
- в пункте 8 обозначьте установку приложений **Microsoft Office Outlook, Microsoft Office Excel , Microsoft Office Word, Microsoft Office Access** и в части **Office Shared Features** обозначьте установку **Галерея клипарт, Помощник Office** и **Visual Basic for Applications**. В установке выберите **Запустить с этого компьютера**;
- в пункте 13 добавьте ярлык для Access.

Создание трансформирующего файла для установки приложения Word

Повторите предыдущие действия с такими изменениями:

- в пункте 5 задайте название файла **Word.MST**;
- в пункте 8 обозначьте установку приложения **Microsoft Office Word** и в части **Office Shared Features** обозначьте установку **Помощник Office**. В установке выберите Запустить с этого компьютера;
- в пункте 13 оставьте ярлык для Word.

Сейчас нужно сказать, что у нас позади самая большая часть работы. В течение этой работы возникли три трансформирующих файла MST, которые вместе с файлами MSI мы будем использовать для определения того, что именно нужно устанавливать.

18.7.6. Объекты групповой политики

Объекты групповой полтики определяют, как будет выглядеть сама установка. Далее мы создадим три объекта групповой политики, которые мы будем применять на подходящих уровнях домена Active Directory.

Создание объекта групповой политики для установки приложения Outlook

Создание групповой политики для установки приложения Outlook производится следующим образом:

1. В компьютере PC001 запустите консоль **Active Directory — пользователи и компьютеры** от имени администратора.
2. Правой кнопкой мыши нажмите на домен (study.local) и отобразите окно свойств.
3. На вкладке **Групповая политика** нажмите **Создать** и дайте имя новому объекту «Install Outlook 2003».
4. Нажмите на кнопку **Параметры** и потом выберите поле **Отключить**: параметры объекта групповой политики не применяются к этому контейнеру. Нажмите OK. Этим вы исключите любую возможность применения данного объекта для компьютеров, входящих в домен.
5. Откройте новый объект для изменений и перейдите к ветви **Конфигурация пользователя\Конфигурация программ.**
6. Правой кнопкой мыши нажмите на **Установка программ** и потом выберите команду **Создать** и далее — **Пакет** (рис. 18.6).
7. В диалоговом окне **Открыть** перейдите к инсталляционному пакету MSI для установки приложений пакета Office. Обратите внимание на то, что вы должны указать сетевой путь (начните с нажатия кнопки **Сетевое окружение** в левой части окна). Потом нажмите **Открыть**.

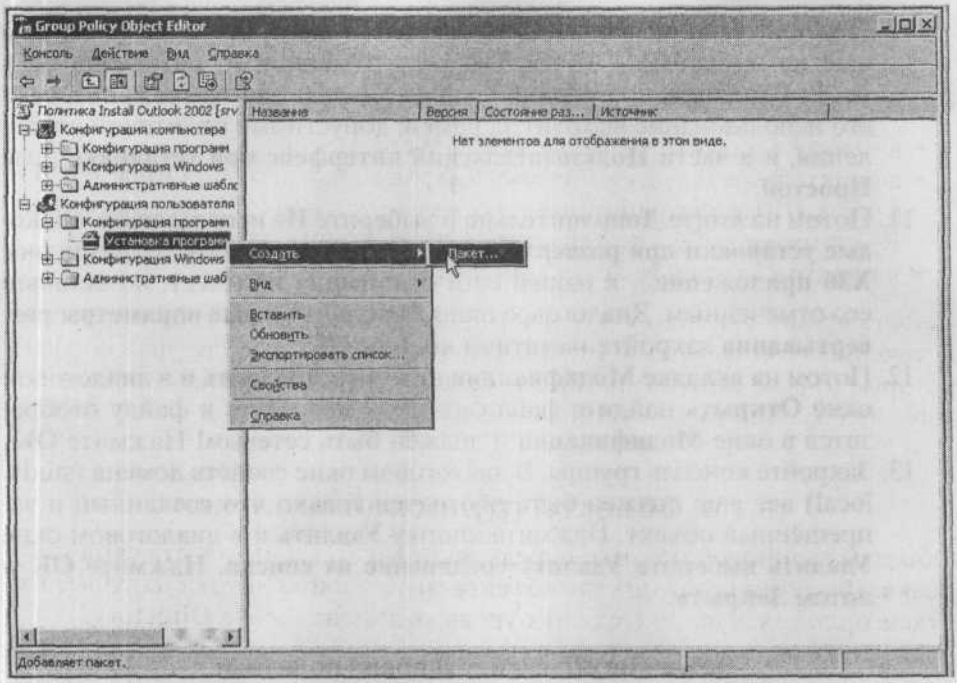


Рис. 18.6. *Добавление в объект групповой политики инсталляционного пакета*

8. В диалоговом окне **Развертывание программ** выберите **Особый** и потом нажмите **OK** (в любом другом варианте пакет MSI нельзя было бы трансформировать при помощи файла MST). Отобразится диалоговое окно с названием приложения с возможностями конфигурации его развертывания.
9. На вкладке **Общие** измените в поле **Название** имя инсталляционного пакета на «Microsoft Outlook 2003».

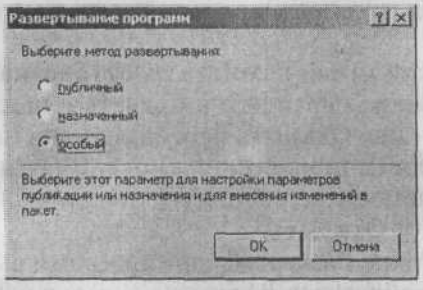


Рис. 18. 7. *Диалоговое окно* ***Развертывание программ***

10. Перейдите на вкладку **Развертывание** и выберите поля (если они ещё не выбраны): в части **Тип развертывания — назначенный**, в части **Варианты проведения** — поле **Удалять это приложение**, если его использование выходит за рамки, допустимые политикой управления, и в части **Пользовательский интерфейс при установке** поле **Простой**.
11. Потом нажмите **Дополнительно** и выберите **Не использовать языковые установки при развертывании**. Поле **Сделать это 32-разрядное X86 приложение**... к нашей сети отношения не имеет, но оставьте его отмеченным. Диалоговое окно **Дополнительные параметры развертывания** закройте нажатием кнопки **OK**.
12. Потом на вкладке **Модификации** нажмите **Добавить** и в диалоговом окне **Открыть** найдите файл `Outlook.MST`. Путь к файлу отобразится в окне **Модификации** и должен быть сетевым! Нажмите **OK**.
13. Закройте консоль группы. В диалоговом окне свойств домена (study.local) всё ещё должен быть обозначен только что созданный и запрещённый объект. Нажмите кнопку **Удалить** и в диалоговом окне **Удалить** выберите **Удалить соединение из списка**. Нажмите **OK** и потом **Закрыть**.

Создание объекта групповой политики для установки приложения Outlook, Word и Excel

Здесь остаётся только напомнить — отделы продаж и маркетинга этими приложениями пользуются ежедневно и нам надо, чтобы ярлык этих приложений сразу же отобразился в меню Пуск.

1. В компьютере PC001 запустите как администратор консоль **Active Directory — пользователи и компьютеры**.
2. Правой кнопкой мыши щелкните по организационной единице Marketing и отобразите окно свойств.
3. На вкладке **Групповая политика** нажмите **Создать** и новый объект параметров назовите «Install Outlook, Word, Excel 2003».
4. Откройте новый объект двойным щелчком и перейдите к папке **Конфигурация пользователя\Конфигурация программ\Установка программ**.
5. Правой кнопкой мыши нажмите на **Установка программ** и потом в контекстном меню перейдите к **Создать** и нажмите **Пакет**.
6. В диалоговом окне **Открыть** перейдите к инсталляционному пакету MSI для установки приложений Office. Внимание! Вы должны действовать при помощи сетевого пути (начните с **Сетевого окружения**). Потом нажмите **Открыть**.
7. В диалоговом окне **Развертывание программ** выберите **Особый** и нажмите **OK**. Отобразится диалоговое окно с названием приложения с вариантами конфигурации его развертывания.

8. На вкладке **Общие** измените в поле **Название** имя инсталляционного пакета на Microsoft Outlook 2003.
9. Нажмите на вкладку **Развертывание** и выберите поля (если они ещё не выбраны): в части **Тип развертывания — назначенный**, в части **Варианты проведения** поле **Удалять это приложение, если его использование выходит за рамки, допустимые политикой управления** и в части **Пользовательский интерфейс при установке** — поле **Простой**.
10. Потом нажмите **Дополнительно** и выберите **Не использовать языковые установки при развертывании**. Поле **Сделать это 32-разрядное X86 приложение...** к нашей сети отношения не имеет, но оставьте его отмеченным. Диалоговое окно Дополнительные параметры развертывания закройте нажатием кнопки **OK**.
11. Потом на вкладке **Модификации** нажмите **Добавить** и в диалоговом окне **Открыть** найдите файл OutlookWordExcel.MST. Путь к файлу отобразится в окне **Модификации** и должен быть сетевым! Нажмите **OK**.
12. Закройте все диалоговые окна и консоли.

Создание объекта групповой политики для установки приложения Word для склада

Напомним, что работники склада используют это приложение время от времени. Поэтому мы не будем отягощать их меню **Пуск**, а просто опубликуем.

1. В компьютере PC001 запустите как администратор **Active Directory — пользователи и компьютеры**.
2. Правой кнопкой мыши щелкните по подразделению Склад (Store) и отобразите диалоговое окно свойств.
3. На вкладке **Групповая политика** нажмите **Создать** и новый объект параметров групповой политики назовите «Publish Word 2003».
4. Раскройте новый объект и перейдите к папке **Конфигурация пользователя\Конфигурация программ\Установка программ**.
5. Правой кнопкой мыши нажмите на **Установка программ** и потом в части **Создать** выберите **Пакет**.
6. В диалоговом окне **Открыть** перейдите к файлу MSI для установки приложений Office. Внимание! Вы должны действовать при помощи сетевого пути (начните с **Сетевого окружения**). Потом нажмите **Открыть**.
7. В диалоговом окне **Развертывание программ** выберите **Особый** и нажмите **OK**. Отобразится диалоговое окно с названием приложения с вариантами конфигурации его развертывания.
8. На вкладке **Общие** измените в поле **Название** имя инсталляционного пакета на «Microsoft Word 2003».
9. Перейдите на вкладку **Развертывание** и выберите поля (если они ещё не выбраны): в части **Тип развертывания — назначенный**, в части **Ва-**

рианты проведения поле **Удалять это приложение, если его использование выходит за рамки, допустимые политикой управления** и в части **Пользовательский интерфейс** при установке — поле **Простой**.

10. Потом нажмите **Дополнительно** и выберите **Не использовать языковые установки при развертывании**. Поле **Сделать это 32-разрядное X86 приложение**... к нашей сети отношения не имеет, но оставьте его отмеченным. Диалоговое окно **Дополнительные параметры развертывания** закройте нажатием кнопки **OK**.
11. Потом на вкладке **Модификации** нажмите **Добавить** и в диалоговом окне **Открыть** найдите файл Word.MST. Путь к файлу отобразится в окне **Модификации** и должен быть сетевым! Нажмите **OK**.
12. Закройте все диалоговые окна и консоли.

Создание объекта групповой политики для установки приложений в дирекции

Дирекция будет располагать следующими приложениями пакета Office — Outlook, Word, Excel и Access.

1. В компьютере PC001 запустите как администратор **Active Directory — пользователи и компьютеры**.
2. Правой кнопкой мыши нажмите на подразделение Дирекция (Managers) и отобразите диалоговое окно свойств.
3. На вкладке **Групповая политика** нажмите **Создать** и новый объект параметров групповой политики назовите «Install Outlook, Word, Excel, Access 2003».
4. Раскрйте новый объект и перейдите к папке **Конфигурация пользователя\Установка программ**.
5. Правой кнопкой мыши нажмите на **Установка программ** и потом в части **Создать** выберите **Пакет**.
6. В диалоговом окне **Открыть** перейдите к файлу MSI для установки приложений Office. Внимание! Вы должны действовать при помощи сетевого пути (начните с **Сетевого окружения**). Потом нажмите **Открыть**.
7. В диалоговом окне **Развертывание программ** выберите **Особый** и нажмите OK. Отобразится диалоговое окно с названием приложения с вариантами конфигурации его развертывания.
8. На вкладке **Общие** измените в поле **Название** имя инсталляционного пакета на «Microsoft AccessWordExcelOutlook 2003».
9. Нажмите на вкладку **Развертывание** и выберите поля (если они ещё не выбраны): в части **Тип развертывания — назначенный**, в части **Варианты проведения** поле **Удалять это приложение, если его использование выходит за рамки, допустимые политикой управления** и в части **Пользовательский интерфейс при установке** — поле **Простой**.

10. Потом нажмите **Дополнительно** и выберите **Не использовать языковые установки при развертывании**. Поле **Сделать это 32-разрядное X86 приложение...** к нашей сети отношения не имеет, но оставьте его отмеченным. Диалоговое окно **Дополнительные параметры развертывания** закройте нажатием кнопки **OK**.
11. Потом на вкладке **Модификации** нажмите **Добавить** и в диалоговом окне **Открыть** найдите файл AccessWordExcelOutlook.MST. Путь к файлу отобразится в окне **Модификации** и должен быть сетевым! Нажмите **OK**.
12. Закройте все диалоговые окна и консоли.

Применение созданного объекта к отделу маркетинга

Маркетинг с точки зрения установки программного обеспечения будет выглядеть точно как отдел продаж. Так что не нужно будет создавать дальнейшие объекты, нужно будет только применить уже существующий объект групповой политики к организационной единице Маркетинг. Выполните следующие действия:

1. В компьютере PC001 запустите как администратор **Active Directory — пользователи и компьютеры**.
2. Отобразите окно свойств организационной единицы `Marketing`.
3. На вкладке **Групповая политика** нажмите **Добавить**. Отобразится диалоговое окно **Добавить ссылку на объект групповой политики**. Нажмите на вкладку **Все**, выберите объект «Install Outlook, Word, Excel 2003» и потом нажмите **OK**.
4. Нажмите **Закрыть**.

Применение созданного объекта для установки Outlook

Приложение Outlook нужно установить всем пользователям, которым оно необходимо для работы. Примените объект, устанавливающий приложение Outlook, к оргединице IT.

1. В компьютере PC001 запустите как администратор **Active Directory — пользователи и компьютеры**.
2. Отобразите окно свойств организационной единицы IT.
3. На вкладке **Групповая политика** нажмите **Добавить**. Отобразится диалоговое окно **Добавить ссылку на объект групповой политики**. Нажмите на вкладку **Все**, выберите объект «Install Outlook, Word, Excel 2003» и потом нажмите OK.
4. Нажмите **Закрыть**.

Установка различных планируемых приложений готова. Теперь пришла пора проверки.

Проверка установок

Проверка установки приложения Outlook 2003.

1. Зарегистрируйтесь на PC001 как пользователь `ITManager1`.
2. При процессе входа вы можете наблюдать диалоговое оно установки программного обеспечения. Это окно отобразится на очень короткое время, поскольку не приводит непосредственно к настоящей установке программного обеспечения, но только лишь к подготовке компьютера и обновлению главного меню.
3. Откройте группу **Пуск → Все программы** и обратите внимание на приложение Microsoft Outlook.
4. Не проводите установку приложения.
5. Выйдите из системы.

Чтобы проверить установку для пользователей отдела продаж:

1. Зарегистрируйтесь на PC001 как пользователь из этого отдела.
2. Откройте группу **Пуск → Все программы** и найдите приложения Microsoft Outlook.
3. Нажмите на файл Microsoft Excel. Произойдёт установка приложения, которая не продлится более двух минут, после чего вас попросят ввести своё имя и инициалы, далее программа запустится.
4. В меню **Справка** нажмите на команду **Справка по Microsoft Excel**. Отобразится информация, что помощь ещё не установлена, с предложением её установить. Нажмите **Да**. После установки справка появится на экране.
5. Проверьте функционирование приложения и закройте его.
6. Выйдите из системы.

Чтобы проверить установку для пользователей со склада:

1. Зарегистрируйтесь на PC001 как пользователь отдела Склад (к примеру, Store1).
2. Откройте группу **Пуск → Все программы** и проверьте, что там нет никаких ярлыков приложений пакета Office.
3. Откройте окно **Установка и удаление программ** и запустите апплет **Установка и удаление программ**.
4. В левой части окна **Установка и удаление программ** нажмите **Установка программы**.
5. Отобразится вариант установки приложения Microsoft Word 2003.
6. Нажмите на кнопку **Добавить**. Запустится установка и отобразится информация об её окончании. Потом в меню **Пуск** появится ярлык, который вы можете использовать для запуска приложения.

Чтобы проверить установку для руководства:

1. Зарегистрируйтесь на PC001 как пользователь из дирекции.

2. Откройте группу **Пуск → Все программы** и найдите приложения Microsoft Office: Microsoft Access, Word, Excel и Outlook.
3. Запустите любое приложение, проверьте его функционирование и потом закройте.

Удаление приложений

1. В окне Панели управления запустите апплет **Установка и удаление программ**.
2. Нажмите на пункт Microsoft Outlook, Word, Excel и Access 2002 и потом нажмите **Удалить**. Может, вы этого и не ожидали, но произойдёт полное удаление приложений. В меню **Пуск**, однако, останутся ярлыки, и после повторного запуска вы снова увидите ссылки на них.
3. Выйдите из системы.

18.7.7. Дополнительная информация к установке приложений с помощью групповой политики

Установка программного обеспечения является одной из самых важных функций в системах Windows 2000/XP/2003. С помощью этой функции можно решить сразу несколько проблем, с которыми администраторы сталкивались и раньше:

- Подготовка к установке выполняется очень быстро.
- Установка происходит автоматически.
- Установить инсталляционный пакет может обычный пользователь.
- Администраторы имеют контроль над тем, кто именно данное программное обеспечение может установить и использовать.
- Администраторы могут заблокировать возможность установки в любой момент.

Для успешной установки и использования этой функции нужно иметь в распоряжении ещё кое-какую информацию.

Удаление инсталляционных пакетов приложений

Если вы хотите удалить возможность установки приложений (например, у одного подразделения), проделайте это в объекте групповой политики следующим образом:

1. На пакет нажмите правой кнопкой мыши и в части **Все задачи** нажмите **Удалить**. Отобразится диалоговое окно **Удаление приложений**, в котором у вас есть два варианта. Немедленное удаление этого приложения с компьютеров всех пользователей удалит у пользователей

это приложение, если оно, конечно, у них есть, при следующем входе в систему, второй пункт (разрешить использование уже установленного приложения, но запретить новую установку) запрещает дальнейшую установку программного обеспечения пользователям.

2. Если вы хотите обеспечить как можно более быстрое удаление установленных приложений, необходимо использовать первый пункт и заставить пользователя сразу же перезагрузить компьютер (если программное обеспечение привязано к компьютеру) или выйти из системы и снова войти. Второй вариант запрещает только новые установки. Пользователи, которые приложение (приложения) уже установили, смогут пользоваться ими и дальше.

Актуализация приложений (например, новая библиотека DLL)

Если у вас в установленном приложении есть ошибка и её исправление заключается в замене одного файла (например, новая библиотека DLL), необходимо от поставщика программного обеспечения получить этот исправленный файл и новую версию файла MSI. После этого действуйте следующим образом:

1. Файлы DLL и MSI скопируйте в инсталляционную папку (перепишите первоначальную версию).
2. Откройте объект групповой политики и перейдите на инсталляционный пакет. Нажмите на него правой кнопкой мыши и в части **Все задачи** нажмите **Развернуть приложение заново**.

Дальнейшие возможности актуализации с использованием файлов MSP, включая практические примеры, вы найдёте в главе 20, «Устанавливаем обновление Service Pack».

18.8. Публикация приложений

Публикация приложений используется на крупных предприятиях, быть может, ещё чаще, чем установка. Опубликованные приложения появляются у пользователей в апплете **Установка и удаление программ** Панели управления.

Такая ситуация может быть, однако, слишком трудной для пользователя. Задайте себе вопрос: кто из пользователей знает, чему служит то или иное приложение? Знают ли пользователи, зачем нужно приложение Adobe Acrobat Reader? Знают ли различия между его версиями?

Необходимо в данном случае создать категории и разделить отдельные приложения. Поступайте следующим образом:

1. Зарегистрируйтесь на SRVR001 как администратор.

2. Откройте объект групповой политики, который применяется для некоторого пользователя.
3. Перейдите в папку **Конфигурация пользователя\Конфигурация программ** и правой кнопкой мыши нажмите команду **Установка программ — свойства.**
4. На вкладке **Категории** нажмите кнопку **Добавить** и задайте название категории. Действия повторяйте для всех категорий, которые вы хотите создать.
5. Нажатием кнопки **OK** закройте диалоговое окно.

Если вы хотите добавить инсталляционный пакет в категорию, отобразите диалоговое окно его свойств и на вкладке **Категории** выберите все категории, в которые должен попасть.

18.9. Модернизация с помощью принципов групповой политики

Групповая политика делает возможным также модернизацию, или апгрейд, приложений (установку новейшей версии). Требованием в такой ситуации является, чтобы и новая версия программного обеспечения была в формате инсталляционного пакета MSI.

Два варианта апгрейда

Существуют два варианта апгрейда:

- **Необходимый.** В момент, когда пользователь запустит существующее приложение, произойдёт автоматически её апгрейд.
- **Не необходимый.** Пользователь может выбрать, какую версию будет использовать. Как только он запустит новую версию, произойдёт автоматический апгрейд.

Планирование апгрейда

На этом этапе нужно определить объекты групповой политики, их применение в действующую инфраструктуру, папки для администраторской установки, конфигурации их полномочий для доступа и изучить документацию к приложениям.

Тестирование установки

Установку программного обеспечения необходимо проверить вне рабочего пространства (вне сети фирмы). Создайте тестовую сеть, соответствующую конфигурации доменного пространства. Следите за тем, чтобы

тестовый компьютер имел такую же конфигурацию, как и компьютеры пользователей в сети.

При тестировании установки используйте обычные учётные записи пользователей. На практике я несколько раз сталкивался со случаями, когда тестирование прошло без осложнений, но в дальнейшем без них не обошлось. Единственным отличием было то, что при тестировании администраторы использовали не обычные доменные учётные записи,, а только учётные записи с полномочиями администратора.

Пилотная фаза

После успешного тестирования установите приложение некоторому количеству пользователей. Чтобы вам из-за этой фазы не менять структуру оргединиц, определите объекты с установками на уровне домена и для их применения используйте принцип фильтрации.

Коррекция плана

На основе напоминаний пользователей и собственных впечатлений от установки приложений в пилотном пространстве проведите, если возможно, коррекцию в плане и потом повторите тестирование на пользователях (если будет нужно).

Постепенная установка

Установка приложений проводите всегда постепенно. И в случае установки объекта групповой политики на уровне домена используйте прежде всего принцип фильтрации, чтобы вы таким образом ограничили приложение на часть пользователей. Не продолжайте, если не будете уверены в безупречном функционировании.

Документация

Весь план и итоговую инфраструктуру подробно задокументируйте. Эта информация будет годиться при любых осложнениях, архивации, при случае обновления инфраструктуры установочных папок на другом компьютере.

Используйте разум

Если вы проведёте установки в рабочем пространстве числом в 1000 компьютеров и на трех из них установка будет неудачной, не ищите проблему в параметрах объекта групповой политики. Скорее всего про-

блема кроется в данном случае в этих трёх компьютерах. Иногда кажется невероятным, сколько энергии, времени и средств способны потратить администраторы на подобные ситуации с целью решения, в общем-то, несущественных проблем.

18.10. Итоги

Существуют различные варианты установки приложений. Средство Групповая политика в доменах с системами Windows 2000/2003 позволяет автоматически устанавливать программное обеспечение для отдельных компьютеров или пользователей. Это средство располагает различными возможностями конфигурации, и для его проведении на практике вам не потребуется дополнительное программное обеспечение. Единственное, что должно быть соблюдено, — это формат устанавливаемого приложения, инсталляционный пакет MSI.

Приложения можно привязывать к компьютерам или к пользователям. В первом случае вы можете сказать, что в данном компьютере будет данное приложение при любых обстоятельствах, даже если в систему войдёт новый пользователь. В другом случае приложение «путешествует» вместе с пользователем и будет в каждом компьютере, в систему которого войдёт пользователь (это касается компьютеров с системами Windows XP Professional/Windows 2000). После добавления приложения в меню Пуск отобразится ярлык данного приложения, установка приложения произойдёт после запуска его пользователем. Моментальную установку (то есть установку сразу после входа пользователя) также можно разрешить (только в доменах с системой Windows Server 2003).

Приложения можно также пользователям публиковать. В этом случае в меню **Пуск** не создаются ярлыки, но пользователи могут опубликованные приложения установить с помощью апплета Панели управления **Установка и удаление программ**. После установки в меню **Пуск** отобразится ярлык приложения. Если опубликовано много приложений и пользователи не ориентируются по названиям, можно определить категории и приложения по ним распределить. Пользователи смогут выбирать исходя из категорий.

Групповая политика делает возможным иметь в своём распоряжении полную информацию о том, где именно какое приложение установлено. Если пользователь выйдет из области действия объекта групповой политики (например, его учётная запись переместится в другую оргединицу), приложение у него автоматически удалится. Администратор имеет возможность приложение в любой момент удалить и обеспечить его автоматическое удаление при следующем входе в систему пользователя.

Основные возможности были представлены в этой главе на конкретном примере установки приложений пакета Office 2003. Мы использовали как добавление, так и публикацию программного обеспечения. Более того, в этом процессе было использовано средство Custom Installation Wizard, который является частью комплекса средств Office 2003 Resource Kit и без которого этот тип установки невозможно определить.

При установке объектов групповой политики всегда действуйте очень осторожно. В случае неудачи неполная установка в пользовательских компьютерах может сильно повлиять на их работоспособность.

Состояние сети

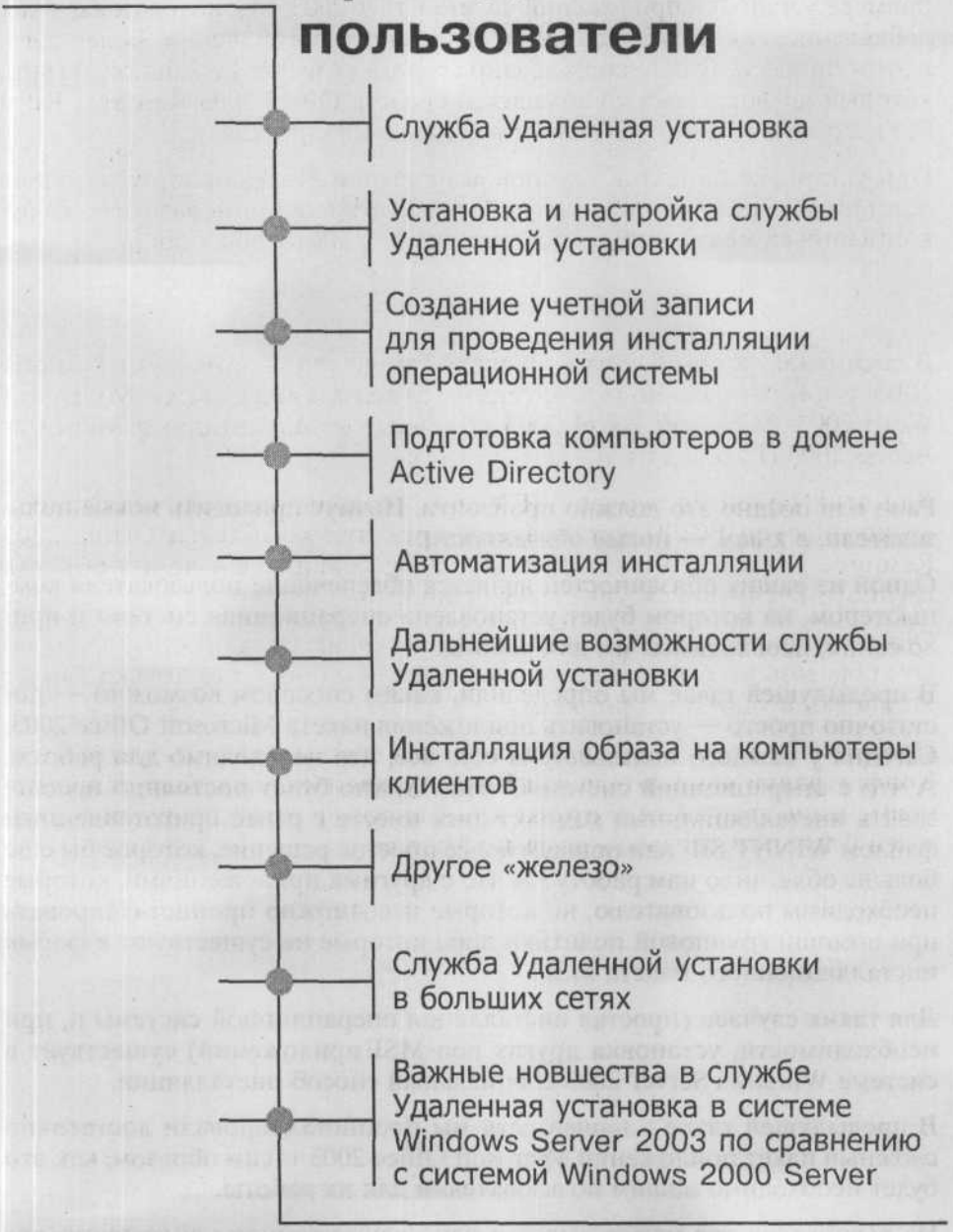
В сети были установлены несколько приложений: Microsoft Outlook 2003 у некоторых пользователей (отдел Склад), даже Microsoft Word 2003, Microsoft Excel 2003 (Продажи и Маркетинг) и Microsoft Access 2003 (Руководство).

Для этих целей на сервере SRVR001 создана установочная папка, на компьютер PC001 установлены средства комплекса Office 2003 Resource Kit и в домене Active Directory появились 4 новых объекта групповой политики, касающиеся установки.

Объект групповой политики для подразделения Склад был изменён таким образом, чтобы на Панели управления был доступен только апплет Установка и удаление программ.

Просмотрите все объекты и в случае, если совсем не используется часть **Конфигурации компьютера** или **Конфигурации пользователя**, запретите применение этой части. Загрузка компьютеров и регистрация пользователей будут проходить значительно быстрее.

Глава 19 Приходят новые пользователи



Рано или поздно это должно произойти. Начнут приходить новые пользователи, а к вам — новые обязанности.

Одной из ваших обязанностей является обеспечение пользователя компьютером, на котором будет установлена операционная система и приложения, необходимые им для работы.

В предыдущей главе мы определили, каким способом возможно — достаточно просто — установить приложения пакета Microsoft Office 2003. Сегодня у каждого пользователя есть все, что необходимо для работы. А что с операционной системой? Нам нужно будет постоянно использовать инсталляционный компакт-диск вместе с ранее приготовленным файлом WINNT.SIF или поищем более простое решение, которое бы еще больше облегчило нам работу? А что с другими приложениями, которые необходимы пользователю, но которые невозможно проинсталлировать при помощи групповой политики либо которые не существуют в форме инсталляционного пакета MSI?

Для таких случаев (простая инсталляция операционной системы и, при необходимости, установка других non-MSI приложений) существует в системе Windows Server 2003 специальный способ инсталляции.

В предыдущей главе в нашей сети мы проинсталлировали достаточно сложный пакет приложений Microsoft Office 2003 таким образом, как это будет необходимо нашим пользователям для их работы.

Из равновесия вас может вывести одно единственное приложение, которое возможно установить только запуском setup.exe. С этим придется потрудиться, обойти все компьютеры, установить под учетной записью администратора и решить проблемы пользователей.

То же самое и с операционной системой. Прежде чем в фирму поступит новый компьютер, он попадет к вам, вы проинсталлируете на него операционную систему и передадите его пользователю. Почему бы это не сделать как-то проще — например, отправить компьютер прямо к пользователю и инсталлировать непосредственно у него? И что если соединить инсталляцию операционной системы и инсталляцию приложения, которые невозможно проинсталлировать при помощи основной группы?

У указанного типа инсталляции, находящейся в системе Windows Server 2003, есть свое название — удаленная установка.

19.1. Служба Удаленная установка

Цель службы Удаленной установки — максимально упростить администраторам начальную подготовку компьютеров. Вместе с тем принимается во внимание политика, применяемая в больших сетях, когда большинство компьютеров приобретается без флоппи-дисковода и привода CD-ROM.

19.1.1. Требования службы Удаленной установки

Для того чтобы пользоваться службой Удаленной установки, необходимо:

- **Active Directory.** Службу Удаленной установки можно использовать только в домене Active Directory. В одноранговых сетях (peer-to-peer) можете о ней забыть.
- **DNS.** В сети должна работать служба DNS. Хотя это везде приводится как особое требование, ясно, что без службы DNS домен Active Directory не может работать.
- **DHCP.** В сети может существовать сервер DHCP, который должен быть настроен для выдачи в аренду IP-адресов клиентских компьютеров.
- Даже компьютеры клиентов не остаются в стороне. Для того, чтобы компьютеры клиентов могли использовать этот тип инсталляции, они должны удовлетворять стандарту PXE (Preboot eXecution Environment). Другими словами, они должны быть оснащены загрузочной памятью boot ROM, при помощи которой они войдут в сеть.

С точки зрения компьютера-клиента, последовательность действий следующая: при включении он получает IP-адрес от сервера DHCP. Затем соединится с сервером службы Удаленной установки и попросит пользователя ввести логин и пароль для подключения. После успешного подключения прочитает с сервера службы Удаленной установки образ установки (либо предложит пользователю выбор из некоторого количества образов) и проинсталлирует его.

Если компьютеры-клиенты не соответствуют стандарту PXE, это еще не означает, что на них нельзя использовать технологию удаленной инсталляции. Удаленная установка содержит в себе файл RBFG.EXE, при помощи которого можно создать загрузочную дискету для такого компьютера.

19.1.2. Подготовка окружения для службы Удаленная установка

Если вы посмотрите на требования, представленные выше, вы поймете, что все они выполнены в нашей сети. Поэтому нам необходимо сделать несколько шагов, прежде чем будет возможно использование Удаленной инсталляции. Речь идет о следующем:

- **Добавление службы Удаленной установки в систему.** Служба Удаленной установки является одним из компонентов системы Windows Server 2003.
- **Конфигурация службы Удаленной установки.** Речь идет о самой важной части всей подготовки службы Удаленной установки. Кроме того, сюда входит подготовка образа операционной системы.
- **Конфигурация службы Active Directory.** В свойствах сервера службы Удаленной установки необходимо сконфигурировать ее «поведение». Кроме того, вы можете настроить и безопасное использование этой службы.

У службы Удаленной установки есть еще одно очень важное требование. Образ для инсталляции на компьютеры должен быть размещен на разделе (логическом диске), отличном от того, где установлена операционная система. Более того, этот раздел должен быть отформатирован файловой системой NTFS.

Во время этой установки сервер превратится в сервер удаленной инсталляции. С него клиенты будут инсталлировать операционную систему и приложения.

Установка сервера службы Удаленной установки включает в себя создание образа операционной системы. Поэтому вам придется задать путь к инсталляционному файлу соответствующей операционной системы. Вы можете указать путь к CD-ROMу, или к общей папке сети, в которой находятся инсталляционные файлы операционной системы.

Служба Удаленной установки в системе Windows Server 2003 делает возможной инсталляцию следующих операционных систем:

- Windows 2000 Professional.
- Windows 2000 Server.

- Windows 2000 Advanced server.
- Windows XP Professional.
- Серверные ОС семейства Windows Server 2003.

В аналогичной службе системы Windows 2000 Server можно было инсталлировать только систему Windows 2000 Professional.

Однако так как наша сеть достаточно маленькая и мы предполагаем использование службы Удаленной установки только для компьютеров клиентов, нам следует подготовиться только к установке системы Windows XP Professional.

19.2. Установка и настройка службы Удаленной установки

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Убедитесь, что присутствует диск **E:**, отформатированный в файловой системе NTFS. Если его нет (хотя во время установки операционной системы на SRVR001 мы его создавали), создайте.
3. В Панели управления щелкните на **Установка и удаление программ.**
4. В окне **Установка и удаление программы** выберите задачу **Установка компонентов Windows**.
5. В диалоговом окне выделите **Служба Удаленной установки (Remote Installation Services)** и нажмите **Далее.**
6. Система Windows Server 2003 выполнит установку данной службы. На время установки необходимо будет вставить инсталляционный компакт-диск.
7. В диалоговом окне **Завершение мастера компонентов Windows** нажмите **Готово.**
8. Перезагрузите компьютер.
9. При загрузке компьютера зарегистрируйтесь как администратор.
10. Выполните команду **Пуск → Выполнить** и в поле **Открыть** введите **ri-setup**. Нажмите **OK.** Запустится Мастер службы удаленной установки. Продолжите нажатием клавиши **Далее.**
11. В диалоговом окне **Местонахождение папки удаленной установки** укажите путь E:\RemoteInstall и нажмите **Далее.**
12. В диалоговом окне **Исходные параметры** оставьте значения по умолчанию и нажмите **Далее.**
13. Теперь вставьте в привод CD-ROM сервера инсталляционный компакт-диск с системой Windows XP Professional.
14. В диалоговом окне **Местонахождение установочных файлов** укажите путь к инсталляционным файлам системы Windows на диске CD-ROM (нажмите на **Обзор** и перейдите в папку). Затем нажмите **Далее.**

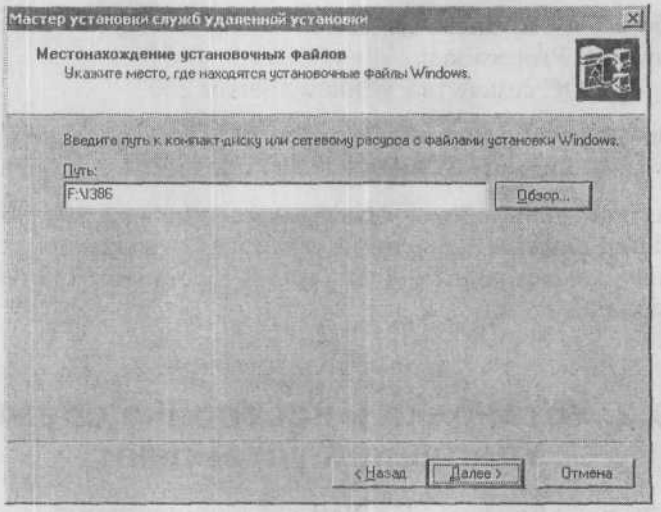


Рис. 19.1. *Путь к инсталляционным файлам системы Windows XP Professional*

15. В диалоговом окне **Имя папки образа установки Windows** укажите имя папки, в которой будет находиться битовая копия инсталляции самостоятельной системы Windows XP Professional (например WXPPRO). Затем нажмите **Далее**.
16. В диалоговом окне **Понятное описание и текст справки** оставьте исходные данные и нажмите **Далее**. Здесь речь идет о данных, тексте, который появится на первом экране при удаленной инсталляции системы на компьютере клиента.
17. В диалоговом окне **Итог установки** просмотрите заданные параметры и затем нажмите на **Готово.** Если хотите какие-то параметры изменить, вернитесь при помощи кнопки **Назад.**
18. Теперь будет выполнена конфигурация службы удаленной установки и инсталляция образа системы Windows XP Professional. Так как копируется содержимое всех инсталляционных файлов Windows XP Professional, процесс установки займет несколько минут.
19. В диалоговом окне с информацией о завершении инсталляции нажмите **Готово**.

Сейчас сервер удаленной инсталляции содержит образ операционной системы. Для того, чтобы инсталляция операционной системы могла начаться, необходимо произвести некоторые действия. Первым шагом будет разрешение службы Удаленная установка.

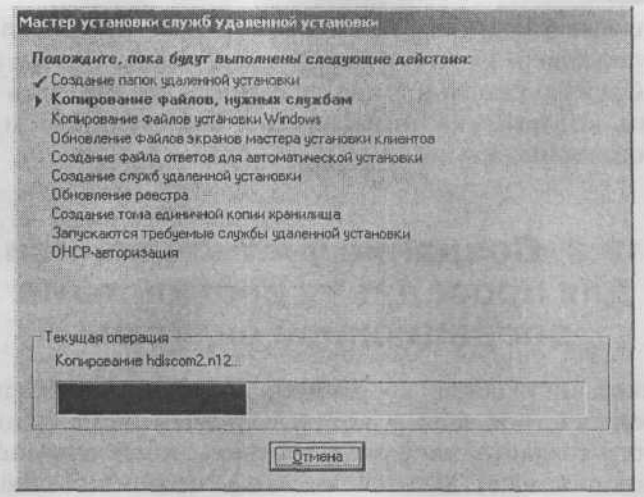


Рис. 19.2. *Конфигурация службы удаленной установки и инсталляция образа системы Windows XP Professional*

19.2.1. Разрешение службы Удаленная установка

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Запустите консоль **Active Directory — пользователи и компьютеры.**
3. Щелкните на **Domain Controllers** и откройте диалоговое окно свойств сервера SRVR001. Убедитесь, что после инсталляции службы Удаленная установка здесь добавилась вкладка **Удаленная установка.**
4. Перейдите на вкладку **Удаленная установка** и установите флажки **Отвечать клиентским компьютерам, запрашивающим обслуживание** и **Не отвечать неизвестным компьютерам-клиентам** (рис. 19.3).

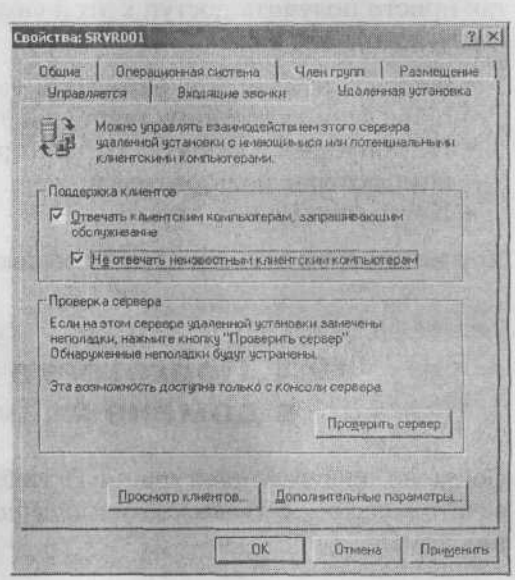


Рис. 19.3. *Свойства сервера удаленной установки*

Установив первый флажок, мы сделали возможным использование службы Удаленной установки. Второй флажок очень важен с точки зрения безопасности. Служба Удаленной инсталляции будет отвечать только тем компьютерам, которые указаны в домене. Каким способом это происходит, мы поговорим чуть позже.

19.3. Создание учетной записи для проведения инсталляции операционной системы

Перед запуском инсталляции операционной системы необходимо указать логин и пароль учетной записи, которые сделают инсталляцию возможной. Для этого создайте, например, учетную запись с именем RIS (Remote Installation Service). Можете создать ее прямо в контейнере Users. Одновременно с созданием снимите отметку с пункта **Требовать смену пароля при следующем входе в систему**.

Так как эта запись нам не понадобится для дальнейшей работы в домене, дальнейшие действия по настройке не нужны.

Безопасность записи RIS

Нужно понимать, что пароль к этой записи будет известен всем пользователям, которые будут производить инсталляцию операционной системы при помощи службы Удаленная установка. Чтобы они не могли так просто получить доступ к этой службе, можно использовать один из следующих методов:

- Запись отключить и разрешать ее использование только на время проведения удаленных инсталляций.
- Не допускать возможность регистрации при помощи этой записи на компьютерах пользователей.
- Постоянно менять пароль.

Другие способы защиты сети и компьютеров вы найдете в главе 22.

19.4. Подготовка компьютеров в домене Active Directory

Согласно нашей конфигурации служба Удаленной установки будет отвечать только *известным компьютерам*. Здесь необходимо сообщить о них домену.

Как было сказано в начале этой главы, службой Удаленной инсталляции могут пользоваться только компьютеры с технологией PXE, либо компьютеры с сетевой картой, поддерживающей данный тип установки. У компьютера, который оснащен технологией PXE, есть уникальный код GUID/UUID (используются оба сокращения). Речь идет о шестнадцатеричном числе, которое можно обнаружить на упаковочной коробке компьютера, на сетевой карте, в документации или в системе BIOS. Вы узнаете его по номеру в формате {921FB974-ED42-11BE-BACD-00AA0-057B223}. Сообщить домену Active Directory о конкретном компьютере означает сопоставить учетной записи компьютера код GUID.

Как поступать в том случае, если компьютер клиента не оснащен загрузочной памятью ROM (не оснащен технологией PXE)? В таком случае GUID код создается из MAC-адреса сетевой карты путем добавления нулей в начале кода так, чтобы он соответствовал 32-значному числу. Например, компьютер с адресом MAC 02-50-56-42-BF-8B получит код GUID {00000000-0000-0000-0000-02505642BF8B}.

Остается только вопрос, как получить необходимые коды и как их назначить учетным записям компьютеров в домене Active Directory. Обнаружение всех необходимых важных кодов (в данном случае код GUID для компьютера с технологией PXE и адрес MAC для остальных компьютеров) лучше оставить поставщику компьютеров. Нужно добавить, что у ответственных поставщиков эта процедура является обязательной и они указывают этот код в документах на компьютер. Тогда вы можете, переписав код, передать компьютер непосредственно пользователю и уже удаленно устанавливать операционную систему без личного присутствия.

19.4.1. Регистрация кодов компьютеров в домене Active Directory

После того как от поставщика вы получите список новых компьютеров с необходимыми кодами, вы можете создать в домене Active Directory их учетные записи. Поступайте следующим образом:

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Запустите консоль **Active Directory — пользователи и компьютеры.**
3. Правой кнопкой мыши щелкните на контейнере **Компьютеры** и в контекстном меню выберите **Создать** и далее **Компьютер.**
4. В поле **Имя компьютера** укажите имя компьютера (соответствующее стандартам организации), рядом с полем **Имя пользователя или группы** нажмите на кнопку **Изменить** и в открывшемся диалоговом окне выбора найдите учетную запись **RIS** (созданную ранее) и затем нажмите **Ок** и **Далее.**

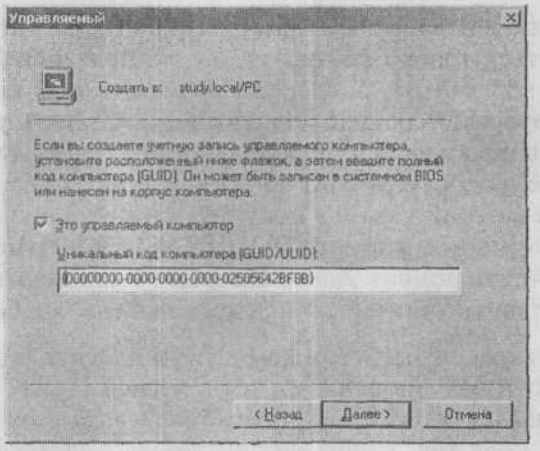


Рис. 19.4. *Присвоение уникального кода новому компьютеру*

5. Отметьте надпись **Это управляемый компьютер** и в поле **Уникальный код компьютера {GUID/UUID}** задайте соответствующий код (включая фигурные скобки, рис. 19.4). Нажмите **Далее.**
6. Оставьте стоять флажок **Любой доступный сервер удаленной установки** и нажмите **Далее.** Второй способ используется для большего количества серверов для удаленной инсталляции и между ними необходимо распределить нагрузку по подготовке компьютеров клиентов.
7. Проверьте заданную информацию и нажмите **Готово**. Таким образом создана учетная запись компьютера и компьютер с этим уникальным кодом возможно будет проинсталлировать при помощи службы Удаленной установки.

Таким же образом необходимо будет создать учетные записи всех компьютеров, которые вы хотите проинсталлировать при помощи службы Удаленной установки.

19.5. Автоматизация инсталляции

А теперь представьте себе, что пользователю вы передадите один из компьютеров, записи которых вы сделали в домене Active Directory. Что произойдет после его запуска?

Так как компьютер оснащен памятью ROM, автоматически после запуска он запрашивает IP-адрес у сервера DHCP, и затем IP-адрес сервера для удаленной инсталляции. Сервер для удаленной инсталляции откроется, и если данный компьютер окажется «знакомым», то появится запрос нажать клавишу F12 для начала процесса установки.

После нажатия клавиши F12 появится приветственное окно сервера удаленной инсталляции, в котором необходимо задать имя, пароль и название домена. Затем появится следующее окно со списком имеющихся образов операционных систем, которые можно установить на компьютер. Выбор, что будет устанавливаться, остается за пользователем.

19.5.1. Настройка автоматического запуска инсталляции

После первого соединения с сервером для удаленной инсталляции компьютер-клиент скачает файл STARTROM.COM, который и позволит пользователю выбрать, что ему установить на компьютер. Так как на сервере для удаленной инсталляции существует только один образ для установки, выбирать не из чего и этот шаг можно пропустить. Для этого замените файл STARTROM.COM на STARTROM.N12:

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Зайдите в папку \\SRVR001\REMINST\OSChooser\i386.
3. Файл STARTROM.COM переименуйте в STARTROM.BAK, а файл STARTROM.N12 переименуйте в STARTROM.COM.

Для того, чтобы пользователь не был сбит с толку вопросами во время установки, необходимо провести следующую настройку объекта групповой политики:

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Запустите **Active Directory — пользователи и компьютеры.**
3. Правой кнопкой мыши щелкните на запись домена (study.local), в контекстном меню выберите команду **Свойства** и перейдите на вкладку **Групповая политика.**
4. Добавьте новый объект с именем **Remote Installation Service,** а в нем добавьте в папку **Конфигурация пользователя\Конфигурация Windows\Служба удаленной установки** и нажмите на **Параметры выбора** в правом подокне.
5. Включите политику **Автоматическая установка.**

Примечание.

Приведенные два способа не являются взаимозаменяемыми. Каждый из них конфигурирует что-то несколько иное и взаимно дополняют друг друга.

Далее, однако, еще нужно решить вопрос автоматической инсталляции самой системы.

Этот тип автоматической инсталляции очень похож на автоматическую инсталляцию системы при помощи файла ответов, с которой мы познакомились в главе 2. Разница будет только в названии файла ответов и его расположении. Способ создания остается почти без изменений.

19.5.2. Настройка автоматической инсталляции с помощью файла ответов

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Запустите **Управление инсталляцией** (это утилита из файла DEPLOY.CAB, который находится на инсталляционном компакт-диске Windows XP Professional или Windows Server 2003 в папке Support\Tools).
3. В **Управлении инсталляцией** выберите создание нового файла ответа, в окне выбора типа установки выберите **Службы удаленной установки (RIS),** в окне **продукт — Windows XP Professional.**
4. В диалоговом окне **Взаимодействие с пользователем** выделите окошко **Полностью автоматическая установка.**
5. В следующих диалоговых окнах задайте те же данные, что вы использовали для создания файла ответов в главе 2. Особое внимание следует уделить следующим установкам:
   - В диалоговом окне **Имя компьютера** отметьте пункт **Автоматически генерировать имя компьютера.**
   - В диалоговом окне **Путь и имя файла** сохраните изначальные установки.
6. Будет создан файл ответов с названием REMBOOT.SIF в папке C:\WINDIST.

19.5.3. Подключение файла ответов к образу удаленной инсталляции

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Запустите **Active Directory — пользователи и компьютеры** и вызовите окно свойств учетной записи компьютера SRVR001.
3. В окне **Удаленная установка** щелкните на **Дополнительные параметры** и перейдите на вкладку **Образы**. Откроется список образов, установленных на данном сервере для удаленной инсталляции (SRVR001).
4. Щелкните на **Добавить** и в диалоговом окне **Новый файл ответов или образ установки** отметьте **Сопоставить новый файл ответов существующему образу.** Затем нажмите **Далее.**

5. В диалоговом окне **Источник файла ответов для автоматической установки** установите флажок **Иное место** и нажмите **Далее**.
6. В диалоговом окне **Выбор образа установки** выделите единственный образ WXPPRO и нажмите **Далее.**
7. В диалоговом окне **Размещение файла ответов** укажите в поле **Путь** путь к файлу ответов, созданному в предыдущем абзаце и сохраненному на сервере SRVR001 (например, \\SRVR001\c$\windist\remboot.sif). Затем нажмите **Далее**.
8. В диалоговом окне **Понятное описание и поясняющий текст** сохраните исходные данные, если они не содержат кириллических символов, иначе содержимое следует заменить латинскими символами. Нажмите **Далее.**
9. Проверьте данные в диалоговом окне **Просмотр параметров** и затем нажмите на **Готово.**
10. Щелчком на **OK** закройте все диалоговые окна. На сервере SRVR001 можете удалить папку с файлом ответов.

К сожалению, этим шагом (конечно же, вынужденным) нарушается вводная часть инсталляции. Сегодня мы можем использовать два способа инсталляции. Служба Удаленной установки не может самостоятельно выбирать, следовательно, необходимо сделать это вручную.

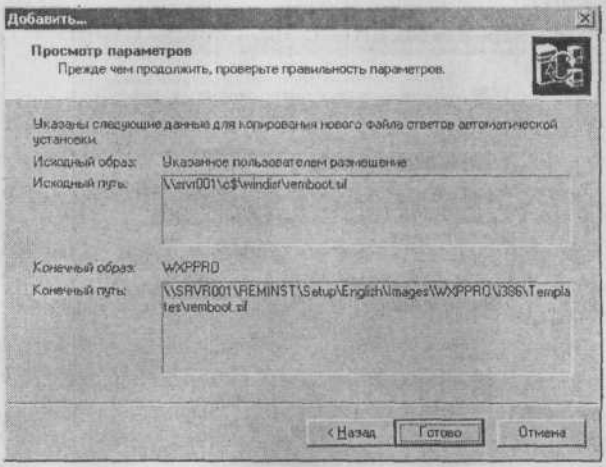


Рис. 19.5. *Итог установки файла ответов существующего образа инсталляции*

19.5.4. Комбинирование образов операционной системы и файлов ответов

Допустим, что существует один образ для инсталляции и два или более файла ответов, которые его модифицируют, и вы хотите быть уверены, что будет осуществлен запуск автоматической инсталляции конкретной комбинации образа и файла. Тогда необходимо закрыть доступ пользователям ко всем остальным файлам ответов.

Как могло показаться, речь идет о текущей установке полномочий на файл (на сервере для удаленной инсталляции), но это не так, и настройку полномочий необходимо провести на учетной записи сервера в домене Active Directory:

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Запустите консоль **Active Directory — пользователи и компьютеры.**
3. На вкладке **Удаленная инсталляция** нажмите кнопку **Дополнительные параметры** и затем кнопку **Образы**. Откроется список образов на данном сервере для удаленной инсталляции (SRVR001).
4. Выделите образ без файла ответов, обеспечивающего автоматическую инсталляцию, обозначенный как **Microsoft Windows XP Professional** и нажмите кнопку **Свойства.**
5. В нижней части диалогового окна **Свойства образа** нажмите кнопку **Разрешения.** Появятся свойства файла ответов.

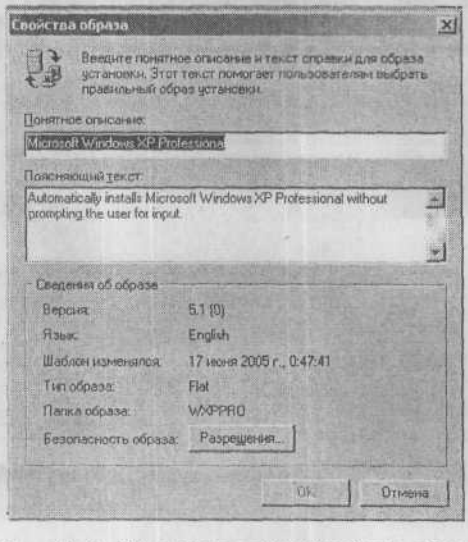


Рис. 19.6. *Диалоговое окно Свойства образа*

6. Щелкните на вкладку **Безопасность.** Нажмите кнопку Дополнительно, отключите наследование разрешений и удалите из списка субъектов доступа группу Authenticated Users.
7. По очереди щелкните на **OK, Отмена, OK** и **OK.**

Примечание.

Как следует из вышеприведенной инструкции, служба Удаленная установка могла бы каждой группе пользователей сопоставить различные комбинации образа и файла ответов.

Приведенная инструкция показывает то, как служба Удаленной установки решает, какой образ может использовать пользователь для инсталляции. Если вам необходимо настраивать установку большего количества образов и различных полномочий, помните, что для регистрации всех пользователей мы выше определяли единственную учетную запись RIS. Вам же потребуется создать несколько таких записей, каждая из которых будет соответствовать конкретной комбинации образа и файла ответов.

19.6. Дальнейшие возможности службы Удаленной установки

Не везде положение так идеально, как у нас. Речь идет о том, что в нашем случае мы все необходимые приложения инсталлируем при помощи объектов групповой политики и поэтому достаточно того, что пользователи при помощи службы Удаленной установки проинсталлируют только операционную систему.

Поэтому вышеприведенная конфигурация, которая действительно обеспечивает автоматическую инсталляцию операционной системы, недостаточна и ее нужно дополнить. Конечно же, мы будем иметь в виду, что проинсталлировать пользователям автоматически операционную систему и приложения быстрее, чем инсталлировать автоматически только операционную систему, а приложения затем инсталлировать постепенно на каждый компьютер.

В следующем примере мы будем исходить из того, что пользователи при помощи службы Удаленной инсталляции будут инсталлировать образ, состоящий из операционной системы и некоего приложения, которое инсталлируется только при помощи программы setup.exe, и его невозможно инсталлировать при помощи групповой политики.

19.6.1. Подготовка компьютера-источника

Компьютером-источником является тот компьютер, содержимое жесткого диска которого позже будет преобразовано в образ и размещено на сервере для удаленной инсталляции. Подготовка состоит из:

- **Инсталляции операционной системы.** Для этого можно использовать службу Удаленная установка.
- **Настройки операционной системы.** Речь идет о выборе местоположения файлов, которые впоследствии скопируются в профиль пользователя по умолчанию. Так как мы используем профиль, находящийся в папке NETLOGON, на практике нужно решить, какой путь указать. Либо удалить профиль в папке NETLOGON и сконфигурировать его на компьютере-источнике, либо оставить его в папке NETLOGON. Разница будет в том, что в первом случае (профиль в папке NETLOGON) это будет касаться первого запуска всех пользователей, во втором случае это будет касаться только пользователей, которые зарегистрируются на данном компьютере.
- **Инсталляции приложений.** Проведение установки всех приложений, которые станут составными частями образа на сервере для удаленной инсталляции.
- **Настройки приложений.** Речь идет об изначальной настройке приложения, которое будет у всех пользователей в том случае, если они будут пользоваться сконфигурированным профилем.

В роли компьютера-источника, как обычно, выступит PC001.

19.6.2. Создание образа и его сохранение на сервере

Создание образа и его размещение на сервере для удаленной инсталляции — дело простое. Но предположим, что вам бы хотелось иметь на сервере для удаленной инсталляции несколько очень похожих образов, которые отличаются только одним приложением. Не жалко отдавать под это много места? Нельзя ли это сделать более разумно?

Система Windows Server 2003 обладает для этого всем необходимым. Правда, еще потребуется наличие файловой системы NTFS и службы хранения единственного экземпляра (Single Instance Store), но первое условие является основным требованием для инсталляции службы Удаленная инсталляция, а служба Single Instance Store является частью службы Удаленная инсталляция.

Служба хранения единственного экземпляра при копировании нового образа следит за тем, нет ли точно такого же файла на сервере для удаленной инсталляции. Если такой файл уже существует, то новый файл не

сохраняется, а создается ссылка на первоначальный файл. Результатом этого является экономия места на диске.

Предположим, что на компьютер PC001 были проинсталлированы все необходимые приложения и компьютер готов к созданию образа. Следуйте дальнейшим указаниям:

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Откройте окно приложения Проводник Windows и перейдите в папку \\SRVR001\RemoteInstall\Admin\i386. Запустите приложение **riprep.exe** (Remote Installation Preparation).
3. Запустится Мастер подготовки удаленной установки. Нажмите **Далее.**
4. В диалоговом окне **Имя сервера** задайте название SRVR001 и нажмите **Далее.**
5. В диалоговом окне **Название папки** укажите название папки, в которой будет размещен образ инсталляции (например, WXPTEL).
6. В диалоговом окне **Краткое описание и подсказка** задайте в поле **Описание** описание инсталляции (например, Windows XP Pro + Apps) и на поле **Подсказка** текст (например, Windows XP Professional Installation with...). Надписи не должны содержать кириллические символы. Затем нажмите **Далее.**
7. В диалоговом окне **Сообщение о совместимости системы** вы можете столкнуться с различными типами сообщений. Нажатиему **Далее** продолжите работу (возможно, придется снова запустить **riprep.exe**).
8. В диалоговом окне **Остановка служб** появится список служб, которые при продолжении будут остановлены. Продолжайте нажатием на **Далее**.
9. В диалоговом окне **Работающие программы и службы** завершите указанные приложения и остановите службы. В противном случае могут появиться ошибки. Затем продолжите нажатием на кнопку **Далее.**
10. В диалоговом окне проверьте заданные параметры. Щелчком на кнопку **Назад** можно вернуться к определенному окну. Если все данные верны, нажмите **Далее.**
11. В диалоговом окне **Завершение мастера подготовки удаленной установки** нажмите **Далее.** Инсталляция будет скопирована на сервер для удаленной инсталляции, и компьютер выключится. При его запуске будет произведена минимальная инсталляция.

19.6.3. Открытие проинсталлированного образа

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Запустите **Active Directory — пользователи и компьютеры.**
3. В свойствах учетной записи компьютера SRVR001 щелкните на вкладке **Удаленная установка** на **Дополнительные параметры.**

4. В диалоговом окне свойств удаленной инсталляции сервера SRVR001 перейдите на вкладку **Образы**. Обратите внимание на проинсталлированные копии.

Если будет нужно автоматически проинсталлировать образ на клиентские компьютеры, необходимо повторить действия создания файла ответа и сделать необходимые исправления для этого файла.

19.7. Инсталляция образа на компьютеры клиентов

19.7.1. Компьютеры, поддерживающие технологии PXE

На этих компьютерах необходимо сконфигурировать в первую очередь загрузку из сети. Если сконфигурирована автоматическая инсталляция, пользователю не нужно будет вводить никакие данные, кроме логина, пароля и названия домена.

19.7.2. Компьютеры, не поддерживающие технологию PXE

В первую очередь такие компьютеры должны иметь флоппи-дисковод. Дальше при помощи RBFG.EXE необходимо создать загрузочную дискету для этого типа запуска. После этого все действия полностью повторяют предыдущий абзац.

После запуска инсталляции дискету нужно вынуть, чтобы после перезагрузки инсталляция могла продолжиться.

Для создания загрузочной дискеты:

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Откройте окно приложения Проводник Windows и перейдите в папку \\SRVR001\REMINST\Admin\i386.
3. Вставьте дискету и в указанной папке запустите **RBFG.EXE.**
4. Щелкните на **Адаптеры.** Откройте диалоговое окно **Поддерживаемые адаптеры**, содержащие список поддерживаемых адаптеров. Убедитесь в том, что указанный список содержит сетевые адаптеры клиентских компьютеров.
5. Щелкните на **Создать диск,** чтобы начать создание загрузочной дискеты.

Примечание.

На дискете будет создан единый файл под названием RIDISK, который будет служить для запуска компьютера и для проведения удаленной инсталляции.

19.8. Другое «железо»

А можно ли проинсталлировать образ исходного компьютера на компьютер с другой материнской платой? Или с другим графическим адаптером? Или на компьютер с другим типом процессора?

Образ, созданный при помощи RIPREP.EXE, можно инсталлировать на компьютер с другой аппаратной конфигурацией, если у них одинаковый HAL (Hardware Abstraction Layer). Если на компьютере-источнике, например, HAL поддерживает технологию ACPI, то то же самое должно быть и на другом компьютере.

Инсталляция образа, созданного при помощи RIPREP.EXE, будет работать, если будет соответствовать хотя бы один из нижеперечисленных пунктов:

- Исходный и новый компьютеры имеют одинаковый уровень HAL.
- Исходный и новый компьютеры имеют однопроцессорный или многопроцессорный уровень ACPI HAL (Advanced Configuration and Power Interface).
- Исходный и новый компьютер имеют однопроцессорный или многопроцессорный уровень APIC HAL (Advanced Programmable Interrupt Controller).

Примечание.

Если вам нужно будет узнать тип HAL на компьютере, найдите в папке %systemroot%\system32 файл HAL.DLL, отобразите его свойства и на вкладке **Версия** в части **Дополнительные сведения** выберите **Исходное имя файла**.

Таким образом решается вопрос годности или негодности конкретной битовой копии для нового компьютера.

19.9. Служба Удаленной установки в больших сетях

О службе Удаленной установки уже было сказано многое, а информации и возможностей конфигурации еще больше. Так как пространство нашей сети очень маленькое и простое, мы использовали только основные конфигурации службы Удаленной установки. В этом параграфе приведена дополнительная информация по использованию службы Удаленная установка.

19.9.1. Как узнать MAC-адрес

В абзаце, который был выше посвящен этому вопросу, было сказано, что информацию о MAC-адресе (в том случае, если компьютер не оснащен технологией PXE) можно получить у поставщика. В противном случае вас ожидает распаковка компьютера, подключение, поиск MAC-адреса, упаковка компьютера и доставка пользователю. Как же получить MAC-адрес компьютера, на котором еще нет операционной системы?

1. В дисковод вставьте загрузочную дискету, созданную при помощи RBFG.EXE.
2. В настройках BIOS смените порядок загрузки так, чтобы загружаться с дискеты, и перезагрузитесь.
3. Дождитесь загрузки программы инсталляции системы Удаленной установки. Так как компьютер не подключен к сети и не связан с сервером для удаленной инсталляции, в окне появится его MAC-адрес.

19.9.2. Размещение сервера для удаленной инсталляции

В сетях, которые содержат большее количество серверов, возможно разделить «роли» между отдельными серверами. В идеале разделение должно было бы выглядеть так (каждый пункт — отдельный компьютер):

- Контроллер домена и служба DHCP.
- Сервер DNS.
- Сервер для удаленной инсталляции.

Для размещения сервера для удаленной инсталляции необходимы следующие правила:

- Служба Удаленной установки не устанавливается на серверы Exchange или SQL. Сервер для удаленной инсталляции слишком перегружает сетевой интерфейс и может вызвать значительное снижение производительности этих систем.

- Сервер для удаленной инсталляции не будет работать в беспроводных сетях. В этих сетях невозможно при помощи службы Удаленной установки инсталлировать компьютеры клиентов, так как беспроводные сети не поддерживают стандарта PXE.
- Сервер для удаленной инсталляции не следует устанавливать в сетях, где уже работают программы аналогичного назначения других производителей.

19.9.3. Несколько серверов удаленной инсталляции

Целью увеличения количества серверов удаленной инсталляции в сети является разделение их обязанностей для совместной инсталляции большего количества компьютеров. На практике было выявлено, что максимальное количество компьютеров, которым сервер удаленной инсталляции способен одновременно предоставлять услуги — 75.

Авторизация сервера

В том случае, если вы в сети используете большее количество серверов для удаленной инсталляции, не забудьте все их авторизовать. В противном случае они не будут соответствовать запросам клиентов и не будут соответственно работать. Авторизация в системе Windows server 2003 происходит во время инсталляции службы Удаленная установка; если это не произошло, необходимо авторизовать сервер вручную.

Ручная авторизация сервера удаленной инсталляции

1. Зарегистрируйтесь на компьютере PC001 как администратор и запустите консоль DHCP.
2. Правой кнопкой мыши щелкните по контейнеру **DHCP** и из контекстного меню выберите команду **Список авторизованных серверов.**
3. В диалоговом окне **Управление авторизованными серверами** на **Авторизовать**, укажите IP-адрес или имя сервера. Нажмите **OK.**

Примечание.

Для открытия сервера Удаленной инсталляции, так же как и для сервера DHCP, вам необходимы полномочия члена группы Enterprise Admins.

19.10. Важные новшества в службе Удаленная установка в системе Windows Server 2003 по сравнению с системой Windows 2000 Server

В качестве важных новшеств можно выделить следующие:

- Поддерживается больше операционных систем — Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced server, Windows XP Professional и семейство Windows Server 2003 (служба Удаленной инсталляции в системе Windows 2000 Server поддерживает только инсталляцию системы Windows 2000 Professional, а после соответствующих изменений также и инсталляцию системы Windows XP Professional).
- Большая безопасность при помощи сокрытия пароля.
- Автоматическая авторизация сервера для удаленной инсталляции во время его настройки (Ri-setup).
- Автоматическое определение HAL целевого компьютера и изменение в соответствии с ним списка образов к инсталляции.
- Поддержка 64-битовой версии системы Windows Server 2003 и Windows XP Professional.

Если в сети не будет использоваться автоматическая инсталляция выбранного образа, и выбор будет оставлен за пользователем, то появится несколько информационных окон. Речь идет о текстовых файлах формата OSCML с расширением OSC (Operating System Chooser).

Эти файлы возможно исправить, особенно информацию, которую они содержат. Пользователям во время удаленной инсталляции откроются следующие файлы:

- **LOGIN.OSC** — окно регистрации.
- **CHOICE.OSC** — возможности инсталляции.
- **OSCHOICE.OSC** — если для инсталляции есть несколько образов, откроется их список.
- **WARNING.OSC** — содержит предупреждение о форматировании жесткого диска компьютера.
- **INSTALL.OSC** — содержит больше информации о компьютере и образе, которые будут инсталлироваться.
- **CUSTOM.OSC** — просит пользователя указать имя компьютера и подразделение, в котором создастся учетная запись компьютера.

В инсталляционных папках находятся и другие файлы OSC, содержащие сообщения об ошибках.

19.11. Итоги

Удаленная инсталляция — очень интересная возможность Windows Server 2003. Она содержит в себе лучшее из двух уже известных вам способов инсталляции — автоматического (необслуживаемого) и Sysprep (возможности инсталлировать заранее настроенную операционную систему с приложениями).

Для успешной работы службы Удаленной установки в сети необходимы службы DNS, DHCP и домен Active Directory. Инсталлировать можно все операционные системы версии от Windows 2000 и выше (кроме версии Datacenter Server). Ее могут использовать компьютеры клиентов, которые поддерживают стандарт PXE или имеют сетевой адаптер PCI.

Чтобы сервер удаленной инсталляции работал, он должен быть авторизован в домене Active Directory, подобно серверам DHCP.

Важной частью службы Удаленной установки является ее конфигурация. Она состоит из инсталляции самой службы и инсталляции образа выбранной операционной системы. Она всегда должна быть на сервере для удаленной инсталляции, так как другие образы, которые инсталлируются на сервер, используют ее файлы.

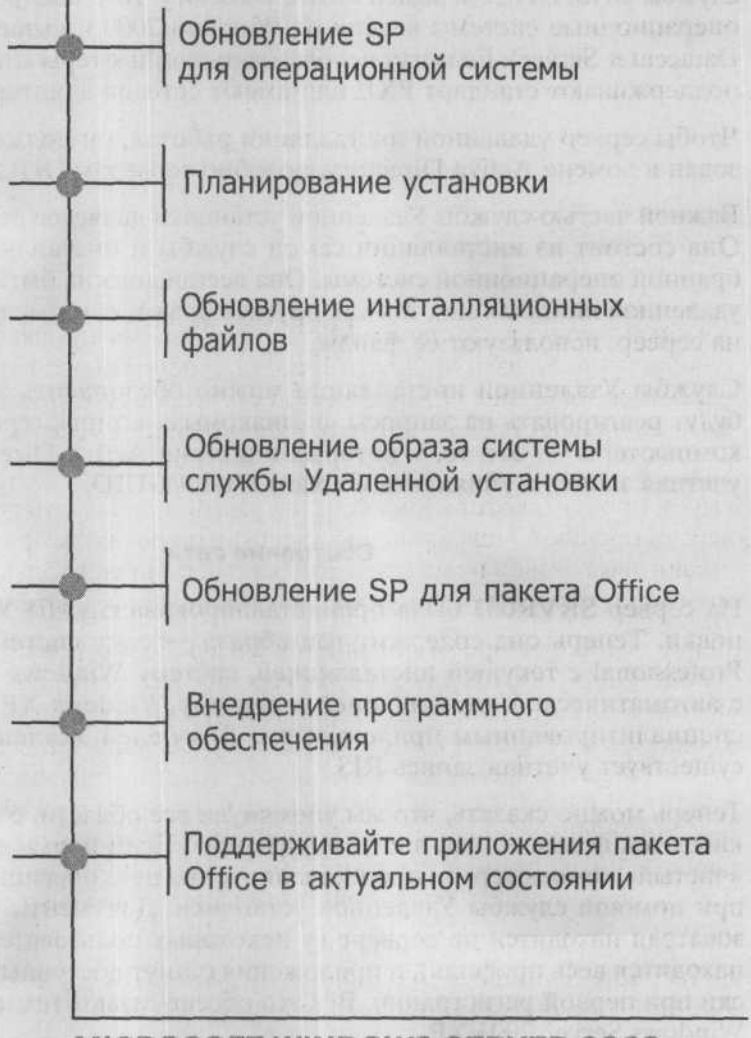
Службы Удаленной инсталляции можно обезопасить так, что они не будут реагировать на запросы «незнакомых» компьютеров. «Знакомые» компьютеры — это те, у которых в домене Active Directory есть своя учетная запись с уникальным кодом UUID/GUID.

Состояние сети

На сервер SRVR001 была проинсталлирована служба Удаленной установки. Теперь она содержит три образа — саму систему Windows XP Professional с текущей инсталляцией, систему Windows XP Professional с автоматической инсталляцией и систему Windows XP Professional со специализированным приложением. Для целей Удаленной установки существует учетная запись RIS.

Теперь можно сказать, что мы упомянули все области, с которыми сталкиваются пользователи в случае «аварии». Если пользователь получает «чистый» компьютер, он проинсталлирует на него операционную систему при помощи службы Удаленной установки. Документы профиля пользователя находятся на сервере (у некоторых пользователей на сервере находится весь профиль), и приложения станут доступными автоматически при первой регистрации. Все это обеспечивают технологии системы Windows Server 2003/XP.

Глава 20 Устанавливаем обновление Service Pack



Каждый продукт компании Microsoft во время производства проходит определенные фазы. Мало кто знает подробности этой «кухни». Большая часть пользователей (и даже администраторов) воспринимает отдельные фазы производства так, как это представляется массам.

Первой стадией является бета-версия — тестовая. Это еще достаточно сырой продукт, который может содержать в себе часть кода предыдущей версии продукта (если, конечно, она существовала), к примеру, некоторые диалоговые окна и подсказки. Эта версия попадает только к так называемым бета-тестерам (участники тестовых программ компании Microsoft).

Через некоторое время появляется следующая версия продукта под названием Beta 2 (и у Beta есть свои версии). Это тот продукт, который уже можно скачать из Интернета, или его можно получить на каких-нибудь конференциях, симпозиумах, семинарах. Обычно эта версия имеет свои ограничения и является бесплатной. Иногда она доступна широким массам, широкому кругу пользователей, которые при использовании ее практически тестируют и имеют возможность отправлять производителю сообщения об ошибках, с которыми сталкиваются при использовании. Таким образом, есть достаточно времени на выявление и исправление ошибок.

Далее может появиться версия с названием RC (Release Candidate). Имеется в виду окончательный продукт. Это именна та версия, которую следует изучать. В большинстве случаев на этих версиях строят официальные курсы, и администраторы имеют возможность подготовиться к использованию и обслуживанию данных продуктов.

Затем настанет новый день, и на рынке появится новая версия. С точки зрения администраторов, разница между конечной и RC версиями состоит в том, что конечная версия полностью поддерживается производителем. Это означает то, что если в предыдущих версиях появляется ошибка, то производители ее исправят и автоматически предупредят в следующих версиях. Если ошибка возникает в новой версии, то исправления создаются как отдельный пакет или публикуется официальная информация по ее устранению.

Так как версии Beta и RC достаточно долго существуют и в них постоянно выявляются и исправляются все ошибки, то с ошибками можно вовсе не столкнуться. Однако операционные системы и приложения компании Microsoft содержат такое большое количество функций, что и конечные версии могут содержать ошибки (несмотря на все усилия производителей).

Через некоторое время, когда исправлений к продукту набирается достаточное количество, производитель может создать отдельный пакет из совокупности исправлений, — обновление. Этот пакет лучше тем, что он содержит полный набор всех предыдущих исправлений и не нужно при переустановке операционных систем и программ устанавливать каждое из них по отдельности. В последнее время составляющие этих обновлений становятся все лучше и приобретают новые свойства. Мы говорим об обновлении Service Pack.

20.1. Обновление SP для операционной системы

Операционная система является основой каждого компьютера, и ее работа может повлиять на целый ряд приложений. В большой сети операционная система (или ее часть) может повлиять на работу приложения, которое проинсталлировано на другом компьютере. На практике мы можем говорить о случае, когда, например, одно из приложений, проинсталлированное на сервере, входящем в домен, требует использовать свойства домена. А если в компоненте операционной системы, отвечающем за домен, есть ошибка, то приложение может вести себя неправильно.

С одной стороны, администраторы могут с нетерпением ждать обновления, исправляющего критические ошибки, с другой, при мысли о том, что инсталляцию нужно будет проделать на всех компьютерах и серверах, мороз бежит по коже. Чем больше поле деятельности, тем больше объем работы. Более того, каждая установка обновления SP требует перезагрузки компьютера, так что можно готовиться к ночной смене.

До системы Windows NT 4.0 такие чувства администраторов были оправданны. Действительно, обновление SP должно было быть установлено на каждый компьютер (конечно же, под наблюдением администратора), более того, при изменении конфигурации системы нужно было обновление переустановить (как, впрочем, и всю операционную систему — прим. редактора). Вместе с системой Windows 2000 на рынок пришла новая возможность автоматической установки при помощи групповой политики. Вскоре после этого изменился формат обновления — его стало возможно интегрировать в службу удаленной установки.

20.1.1. Где взять обновление

Обновление Service Pack пользователи соответствующей операционной системы получают бесплатно. Поэтому не будет проблем с ее поиском. У вас есть на выбор несколько возможностей:

- **Диск CD-ROM с обновлением Windows XP SP1 от компании Microsoft.** Имеется в виду диск CD-ROM, который содержит не только обновление, но также информацию по его проведению, включая другие необходимые настройки операционной системы. Данный диск можно приобрести у официальных дилеров программных продуктов компании Microsoft или заказать на сайте www.microsoft.ru. Во втором случае вам придется оплатить расходы по пересылке.
- **Дополнительный компонент программного обеспечения.** Компании, использующие некоторые типы мультилицензионных программ, получают подписку на инсталляционные диски с приложениями SP (не только для операционных систем) как составляющую часть своей лицензии.
- **Специальные программы компании Microsoft.** Подписчики специальных программ компании Microsoft, таких как MSDN или TechNet, получают все обновления на CD-ROM или DVD в рамках регулярных месячных поставок.
- **Скачивание обновления из Интернета.** Речь идет о самом часто используемом и самом быстром способе получения обновления. В этом случае вы можете быть уверены в том, что скачиваете самую последнюю версию. Если вам понадобится полная информация об обновлении, ее нужно скачать отдельно. С другой стороны, можете быть уверены, что вся эта информация актуальна.
- **Диски CD-ROM (DVD) с выставок, семинаров или из журнала.** Речь идет о часто используемом источнике получения обновлений, изменений и технических материалов. Если же вы не уверены в «происхождении» диска, советуем перед его использованием произвести антивирусную проверку файлов.

20.1.2. Языковые версии

Обновление SP для системы Windows XP отличается для каждой локализованной версии системы. Необходимо из Интернета скачать нужную версию, подходящую именно для вашей системы.

Примечание редактора.

Если у вас английская версия операционной системы с установленным русским пакетом интерфейса, вы должны использовать обновление для изначальной локализации системы, т. е. английское. Правильно будет сначала удалить языковой пакет, затем установить обновление, а потом заново установить русский язык.

С точки зрения необходимости локализовать каждое обновление (в конце концов, любое исправление), вы всегда в первую очередь столкнетесь с обновлением для языковой версии EN. Версий для других языков долго ждать не придется, они появляются в течение нескольких дней.

Если вы будете устанавливать, например, языковую версию EN обновления SP на систему Windows XP Professional RU, установка прервется и сообщит об ошибке.

20.1.3. Типы установки

На обновление SP можно посмотреть как на обычное приложение, которое можно установить несколькими способами. Каждый способ более или менее выгоден в разных условиях, но в каждом случае достаточно возможностей для того, чтобы администратор выбрал самый удобный для него способ.

Установку можно произвести двумя способами:

- Установка обновления отдельно от системы.
- Установка операционной системы с интегрированным обновлением.

Установка обновления отдельно от системы

Имеется в виду тип установки, который знают все администраторы. Это способ, когда устанавливают обновление SP систем семейства Windows на компьютеры с уже установленными операционными системами.

Установка операционной системы с интегрированным обновлением

В главе 2 мы познакомились с автоматической установкой системы Windows XP Professional. Инсталляционные файлы в этом случае могут

быть размещены на компакт-диске или в общей папке в сети. Интеграция обновления в установку операционной системы подразумевает обновление инсталляционных файлов. На оригинальном диске CD-ROM, понятно, этого сделать нельзя; нужно создать собственный диск CD-R или CD-RW.

В предыдущей главе мы познакомились с другой возможностью установки — удаленной установкой. Здесь также можно произвести обновление файлов, которые находятся на сервере RIS.

Интегрированная установка означает, что на «чистый» компьютер устанавливается уже обновленная операционная система.

А теперь рассмотрим подробнее возможности установки относятся к установке обновления отдельно от системы. На компьютере уже должна быть установлена операционная система.

Итак, в сфере нашего внимания будут:

- Установка с диска.
- Установка по сети.
- Установка с помощью продукта SMS.
- Установка при помощи групповых политик.

Установка с диска

При этом способе установки в первую очередь происходит распаковка инсталляционных файлов на диск компьютера. Только потом будет запущена установка обновления Service Pack. Действия должны быть следующими:

1. Вставьте в привод компакт-диск с обновлением Service Pack или скопируйте файл обновления (XPSP_.exe где _ означает версию — 1, 2 и т. д.) на жесткий диск.
2. Остановите работу антивирусных программ и заархивируйте важные данные.
3. Запустите файл **XPSP_.exe.** Так как речь идет о сжатом файле, произойдет его распаковка во временную папку на диске С.
4. Произойдет автоматический запуск установки обновления.
5. Перезагрузка компьютера. Перезагрузка не обязательна (ее можно отменить), но без нее произведенные изменения не вступят в силу.

При запуске файла XPSP_.exe вы можете задать ключи и таким образом внести изменения в установку. Чаще всего используемые ключи приведены в таблице 20.1.

Ключи для запуска XPSP_.exe и Update.exe *Таблица 20.1*

Параметр	Функция
/help	Вывод справки по ключам, используемым для установки обновления
/quiet	Фоновый режим. Полное сокрытие процесса установки обновления от пользователя
/passive	Необслуживаемая установка. Процесс установки будет отображен, но он не потребует вмешательства пользователя
/uninstall	Удаление обновления и возврат системы в исходное состояние
/norestart	Отмена требования перезагрузки системы после установки
/forcerestart	Безусловная перезагрузка системы после установки
/l	Вывод списка установленных обновлений и исправлений
/n	Не сохранять копии изменяемых файлов. Если у вас мало места на диске и вы уверены, что вам не будет необходимо удалять обновление, можете использовать этот ключ
/f	Принудительно закрыть другие программы перед перезагрузкой
/integrate:<путь>	Добавить обновление в инсталляционные файлы, расположенные в указанном месте. Таким образом будут подготовлены инсталляционные файлы операционной системы с интегрированным обновлением
/d:<путь>	Сохранить копии файлов в указанную папку

Установка с диска является стандартным способом установки обновления Service Pack дома и в малых сетях. Также ее можно использовать в том случае, когда необходимо инсталлировать обновление только на один компьютер.

Установка по сети

Этот способ установки очень похож на предыдущий. Самая большая разница заключается в том, что распаковка инсталляционных файлов обновления произойдет в общей папке в сети и на компьютер файлы будут устанавливаться прямо из этой папки.

Процесс установки выглядит следующим образом:

1. Подготовка инсталляции — заключается в распаковке файлов в папку инсталляционного сервера при помощи команды

```
XPSP_.exe /X:<путь к папке> /U
```

Примечание.

Параметр X произведет только распаковку инсталляционных файлов обновления без последующего автоматического запуска update.exe. <путь к папке> — это путь к папке, в которую распаковываются инсталляционные файлы.

2. Остановка антивирусной программы компьютера и архивация важных данных.
3. Запуск установки.
4. Перезагрузка компьютера.

Перезагрузки касается примечание, приведенное выше. Инсталляционную программу **update.exe** можно запустить с ключами, приведенными в таблице 20.1.

Выгодой этого типа инсталляции является однократная распаковка инсталляционных файлов. Остальные компьютеры затем производят установку запуском инсталляционной программы из этой папки.

Установка при помощи продукта SMS

Информация о данном типе установки выходит за рамки этой книги. Единственная важная информация для администраторов, использующих этот тип установки — необходимо использование SMS 2.0 с обновлением Service Pack 4.

Установка при помощи групповой политики

После распаковки файла XPSP_.exe в подпапке **update** окажется файл UPDATE.MSI. Речь идет о стандартном инсталляционном пакете службы системы Windows, установке которого была посвящена глава 18. Установка с использованием инсталляционного пакета приведена далее.

Если мы сравним возможности различных типов установок, то поймем, что для нашей сети самым оптимальным будет использование установки при помощи параметров групповой политики. Сеть располагает всем необходимым — есть домен Active Directory и объект групповой политики Установка программ.

20.2. Планирование установки

При планировании инсталляции нужно обратить внимание на то, что речь идет о вмешательстве в конфигурацию каждого компьютера. Необходимо обеспечить сохранение исходных копий всех изменяемых файлов, а также поэкспериментировать на отдельном компьютере с приложениями после установки обновления. Не забудьте, что если инсталляция пройдет некорректно, то пользователи могут столкнуться с проблемами во всех приложениях.

Далее нужно решить, к какой организационной единице в домене Active Directory будем применять объект групповой политики инсталляции об-

новления. Уровень домена не подходит, так как в нашем случае инсталляция коснулась бы также сервера SRVR001 с системой Windows Server 2003. Однако ранее мы создали организационную единицу «Компьютеры», содержащую все рабочие станции. Ее мы и можем использовать.

Если в вашей сети присутствуют компьютеры не только с системой Windows XP Professional, вам необходимо произвести разделение контейнера, содержащего все компьютеры сети. В этом случае установка соответствующих обновлений для каждого вида операционной системы не вызовет сбоев в работе сети.

Таким образом инсталляция обновления SP произойдет при следующем включении компьютера. Так как данный процесс займет некоторое время, об этом необходимо сразу предупредить пользователей, и если у вас в сети достаточно большое количество компьютеров, надо обеспечить распределение установки приложения по времени, чтобы не произошло перегрузки инсталляционного сервера.

Подготовка инсталляционной папки

На сервере SRVR001 у нас создана общая папка InstallApp пока что с одной подпапкой, содержащей инсталляционные файлы пакета Office. Почему бы не использовать эту папку для размещения инсталляционных файлов обновления SP системы Windows XP Professional? Однако нужно убедиться, что к инсталляционным файлам имеют доступ компьютеры в сети.

Распаковка инсталляционных файлов

1. Зарегистрируйтесь на компьютере SRVR001 как администратор.
2. Установите компакт-диск с обновлением SP для системы Windows XP Professional.
3. В диалоговом окне **Пуск → Выполнить** введите команду

```
F:\XPSP_.EXE/X: C:\InstallApp\XPSP_.EXE /U OK
(F: здесь – обозначение компакт-диска).
```

Примечание.

Если в пути к инсталляционной папке есть пробел, необходимо весь путь заключить в кавычки.

4. Автоматически откроется папка XPSP_. Отобразите ее свойства и перейдите на вкладку **Безопасность**. Добавьте в список субъектов доступа группу **Domain Computers** с правами **Чтение** и **Чтение и выполнение.**

Создание объекта групповой политики

Для создания объекта групповой политики:

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Запустите **Active Directory — пользователи и компьютеры.**
3. Отобразите свойства контейнера **Computers**.
4. На вкладке **Групповая политика** щелкните на **Создать** и дайте название новому объекту групповых политик Install XPSP_.
5. Щелкните на новый объект и нажмите **Изменить.** Перейдите в папку **Конфигурация компьютера\Конфигурация программ\Установка программ.**
6. Правой кнопкой мыши щелкните на **Установка программ** и в пункте **Создать** щелкните на **Пакет.**
7. В окне **Открыть** перейдите в папку на сервере, где находится распакованный файл UPDATE.MSI.
8. В диалоговом окне **Развертывание программ** оставьте режим **назначенный** и нажмите **OK.**
9. Закройте окно групповых политик и откройте свойства организационной единицы «Компьютеры».
10. Перейдите на вкладку **Фильтр WMI**, установите переключатель в положение **Следующий фильтр** и нажмите кнопку **Обзор и управление.** Откроется диалоговое окно **Управление фильтрами WMI** (рис. 20.1). Нажмите **Подробно.**

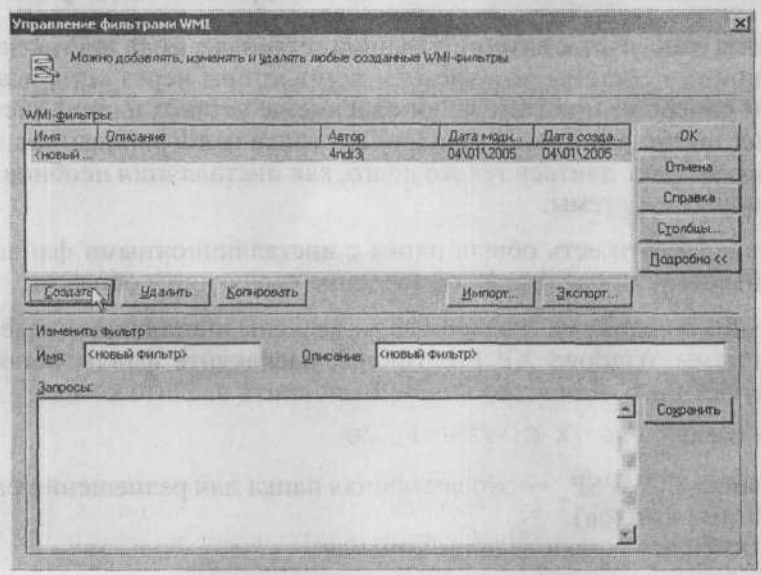


Рис. 20.1. *Диалоговое окно* ***Управление фильтрами WMI***

11. Нажмите кнопку **Создать**. В части **Изменить фильтр** (нижняя часть диалогового окна) укажите имя **Only Windows XP Professional** и в поле **Описание** задайте описание фильтра (например **For Windows XP Professional**). В поле **Запросы** затем укажите следующий фильтр:

```
Root\CimV2; Select * from Win32_OperatingSystem
where BuildNumber = "2600"
```

12. Нажав на кнопку **Сохранить**, сохраните фильтр. Закройте диалоговое окно.
13. Щелчком на **OK** закройте диалоговое окно свойств объекта групповой политики Install XPSP_.
14. Закройте все диалоговые окна.

Объект обновления Service Pack для системы Windows XP Professional теперь готов к использованию. После перезагрузки компьютера PC001 должна произойти инсталляция программного обеспечения.

По окончании инсталляции появится обычное окно регистрации пользователя. В окне **Установка и удаление программ** можете увидеть наличие обновления Windows XP Service Pack _. Информация об обновлении системы так же будет изображаться в диалоговом окне свойств системы — в панели управления выберите элемент **Система**.

20.3. Обновление инсталляционных файлов

Этот метод относится к интегрированной установке. Если инсталлируются операционные системы на «чистые» компьютеры через сеть, возможно простым способом произвести обновление не установленной системы, а исходных инсталляционных файлов. Итоговая интегрированная инсталляция затем будет длиться так же долго, как инсталляция необновленной операционной системы.

Если в вашей сети есть общая папка с инсталляционными файлами системы Windows, проведите ее обновление следующим образом:

1. В общую папку на сервере, где размещены инсталляционные файлы системы Windows XP Professional, распакуйте файлы обновления Service Pack. Для этого в окне **Выполнить** введите команду

```
D:\XPSP_.exe /X C:\TEMPSP_ /U
```

   (папка TEMPSP_ — это временная папка для размещения распакованных файлов).
2. После распаковки введите команду:

```
C:\TEMPSP_\update.exe /S:C:\WXPPRO
```

(папка WXPPRO содержит инсталляционные файлы системы Windows XP Professional.).

3. Удалите папку TEMPSP_.

Каждая следующая инсталляция операционной системы будет включать обновление Service Pack.

20.4. Обновление образа системы службы Удаленной установки

Служба Удаленной установки, которой мы посвятили главу 19, не предполагает включения обновления Service Pack в существующие образы.

20.4.1. Образ Risetup

Этот источник установки невозможно напрямую обновить при помощи Service Pack. Но можно сделать новый образ из обновленных инсталляционных файлов Windows XP.

20.4.2. Образ Riprep

Образ Riprep точно отвечает конфигурации некоторого компьютера и здесь тоже нельзя просто провести обновление. Нужно заново сделать образ с компьютера, на котором было установлено обновление SP.

Не забудьте после добавления обновленного образа удалить предыдущую версию. Основное правило и требование службы Удаленной установки: на сервере для удаленной инсталляции должен существовать хотя бы один образ Risetup (в противном случае служба Удаленной установки не будет работать).

20.5. Обновление SP для пакета Office

Пакет Office не является операционной системой и устанавливается он не средствами службы Удаленной установки, а через объект групповой политики.

Обновления SP операционной системы компания Microsoft создает как накопительный пакет. Каждое последующее обновление включает в себя все предыдущие. Такое положение во многом облегчает работу администраторам и экономит время. Подобным образом созданы обновления

операционных систем и серверных продуктов. К сожалению, это не касается обновлений пакета Office.

Разностные обновления являются полной противоположностью накопительным. Если у вас будет продукт, к которому прилагается 5 разностных обновлений, приготовьте себе кроме всех инсталляционных дисков чашку кофе и хорошую книгу. У вас будет достаточно времени на все это во время инсталляции.

В первую очередь вам нужно будет проинсталлировать сам продукт и затем одно обновление за другим. Типичным представителем продукта, для которого не выпускаются накопительные обновления, является пакет Office.

На сегодняшний день для пакета Office 2003 существует одно обновление Service Pack (в предыдущей версии Office оно называлось Service Release).

20.5.1. Где взять обновление

Эти действия очень похожи на приведенные выше. Самым простым способом будет скачать обновление Service Pack из Интернета. Вот адрес, где найдется все необходимое: http://office.microsoft.com/download. Скачивайте правильные обновления. Так же, как и с операционной системой, у обновления пакета Office есть свои языковые версии.

20.5.2. Тип обновления

Все обновления выполнены в двух различных версиях. Одна из них — клиентская, другая — администраторская.

Клиентское обновление

Этот тип обновления предназначен для прямого запуска на конкретном компьютере, где вы регистрируетесь под именем администратора. Во время инсталляции может потребоваться наличие инсталляционного компакт-диска с пакетом Office 2003. Принцип действия такой, что после запуска произойдет обновление всех важных файлов на компьютере клиента.

Администраторское обновление

Этот тип обновления предназначен для больших сетей, где была проведена инсталляция приложений пакета Office из подготовленной администраторской инсталляции. Это обновление содержит, кроме клиентской части, еще и другие возможности, которые позволяют обновить администраторскую инсталляцию на сервере.

Что необходимо для инсталляции обновления

Кроме знания, как все провести, вам потребуется сама администраторская версия обновления Service Pack в нужной языковой версии, и физический доступ к компьютеру SRV001.

Необходимость тестирования

Работа с приложениями пакета Office для многих администраторов составляет существенную часть их обязанностей. Поэтому очень важно, чтобы действия по инсталляции были хорошо освоены, проверены в лабораторных условиях и с точки зрения их влияния на работу пользователей. Поэтому не проводите сразу инсталляцию на рабочем месте, а протестируйте ее сначала на паре выделенных компьютеров.

Обновление приложений Office невозможно удалить. Поэтому очень важно перед проведением инсталляции все тщательно протестировать. Единственная возможность вернуть назад исходную версию, — это заново создать администраторскую инсталляцию.

Подготовка к инсталляции обновления

1. Зарегистрируйтесь на компьютере SRV001 как администратор.
2. Создайте временную папку (например, TEMPSP_, где _ — номер обновления). Не важно, где она будет расположена, главное, чтобы не на системном диске.
3. Поместите в нее файл Office2003SP_.EXE.
4. В окне **Пуск** → **Выполнить** введите путь к файлу обновления с ключом /**c**. На экране должно появиться окно лицензионного соглашения.
5. Затем укажите место для распаковки файлов — рекомендуем такую же временную папку (C:\TEMPSP_).

В эту папку будут распакованы файлы для обновления. Главные установочные файлы имеют расширение MSP.

20.5.3. Применение обновления к администраторской инсталляции

Если у вас есть файл MSP и вам нужно его применить к инсталляционному ресурсу, принцип действия везде будет одинаковым. Поэтому помните об этом, он может понадобиться и при инсталляции совсем других продуктов.

1. Зарегистрируйтесь на компьютере SRVR001 как администратор.

2. В окне **Пуск → Выполнить** введите:

```
msiexec /p "C:\TEMPSP1\OWC11SP1FF.MSP" /a "\\SRVR001\
InstallApp\Office 2003\OWC11.MSI" SHORTFILENAMES=TRUE
```

3. Откроется диалоговое окно установки **Microsoft Office 2003 Web Components** с лицензионным соглашением. Согласитесь с условиями лицензии и продолжите нажатием на кнопку **Инсталлировать (Install)**.
4. В инсталляционной папке D:\InstallApp\Office 2003 некоторые файлы обновятся. После окончания инсталляции откроется диалоговое окно, которое закройте кнопкой **OK.**
5. В окне **Пуск → Выполнить** введите:

```
msiexec /p "C:\TEMPSP1\MAINSP1FF.MSP" /a "\\SRVR001\
InstallApp\Office 2003\PRO11.MSI" SHORTFILENAMES=TRUE
```

Исходя из размера этого файла, можно ожидать, что теперь обновление займет больше времени, чем в предыдущем случае. Инсталляция пройдет автоматически. По ее окончании откроется диалоговое окно, которое закроете кнопкой **OK**.

20.6. Внедрение программного обеспечения

Мы произвели обновление администраторской инсталляции пакета Microsoft Office 2003, с которой уже инсталлируются другие компьютеры. Не важно, сколько компьютеров-клиентов, 10, 100 или 1000, инсталляционный источник у них один. Но нужно сделать еще один шаг — пользователям, которые свои приложения уже проинсталлировали, нужно сказать, что их нужно проинсталлировать снова. Это можно сделать в домене Active Directory следующим образом:

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Запустите **Active Directory — пользователи и компьютеры.**
3. Отобразите свойства подразделения Shop.
4. На вкладке **Групповая политика** выберите объект групповой политики, при помощи которого инсталлируются приложения пакета Office 2003 для пользователей из этого подразделения, и нажмите **Изменить.**
5. Перейдите в папку **Конфигурация пользователя\Конфигурация программ** и нажмите на **Установка программ.**
6. Правой кнопкой мыши щелкните по значку инсталлируемого программного обеспечения и в части **Все данные** нажмите на **Снова загрузить приложение.** На следующий вопрос ответьте щелчком на **Да.**

7. Эти действия повторите для всех остальных групповых политик, использующих одинаковый инсталляционный источник (в других подразделениях или на уровне всего домена).

Если на компьютере пользователя приложение уже было инсталлировано (то есть пользователь уже запускал его), его обновление будет установлено во время следующей регистрации пользователя в системе. Из-за этого процесс регистрации займет несколько больше времени. По окончании регистрации пользователь может загрузить приложение и сразу работать. Если в обновлении нет новых возможностей, пользователь может даже не увидеть никаких изменений в своей работе.

Если пользователь запустит приложение первый раз, то запустится его инсталляция. Разница будет в том, что теперь инсталлироваться будет уже обновленное приложение.

20.7. Поддерживайте приложения пакета Office в актуальном состоянии

Если вы хотите иметь свои приложения полностью функциональными и безопасными, необходимо устанавливать новые обновления. Однако для поддержания приложений в этом состоянии ежедневно требуется устанавливать не только обновления Service Pack, но и текущие исправления Hotfix.

Текущие исправления нельзя найти нигде кроме как в Интернете на страницах компании Microsoft. Подобно обновлению Service Pack, и эти исправления существуют в двух формах. Первая — клиентская — предназначена для прямой инсталляции на конкретный компьютер, вторая — администраторская — предназначена для применения к установочным файлам приложения. Прежде чем вы решите установить исправления, проверьте их сначала на отдельном компьютере.

Здесь тоже нужно следить за правильностью языковой версии. Если вы по ошибке попытаетесь установить исправление на другом языке, инсталляционная программа автоматически остановится.

20.8. Итоги

Инсталляция обновления Service Pack является необходимостью для администратора, который заинтересован поддерживать программное обеспечение в локальной сети в безопасности, функциональным и актуальным. Эти обновления компания Microsoft выпускает как для опе-

рационных систем клиентских машин, так и для серверных продуктов и других приложений.

У обновления SP есть несколько способов инсталляции. Один из самых простых методов — инсталляция программного обеспечения при помощи групповой политики. Речь идет об изменении объекта групповой политики (подходит и для обновления операционной системы), либо об обновлении администраторской инсталляции (для пакета Office).

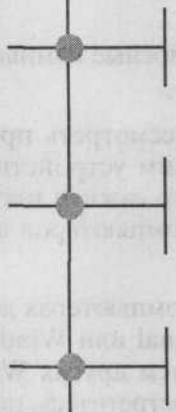
Тогда как обновление SP для системы Windows XP Professional можно удалить, обновление для пакета Office удалить нельзя. Поэтому требуется тщательное тестирование перед его применением.

Компания Microsoft выпускает, кроме того, также текущие исправления. Тогда как у этого типа обновлений, предназначенных для операционной системы, не существует возможности ее инсталляции при помощи объекта групповой политики, у исправлений для пакета Office это возможно. Для этого есть файл MSP для администраторской инсталляции.

Состояние сети

В сети существует обновленная администраторская инсталляция приложений пакета Office на сервере SRVR001. Все пользователи систем Windows XP Professional, таким образом, имеют инсталлированное обновление SP1 и пользуются приложениями пакета Office с обновлением SP2.

Глава 21 Временные подключения к сети. Использование портативных компьютеров (ноутбуков)



Наше предприятие решило закупить переносные компьютеры. Надеемся, для администраторов.

Эта глава не ставит перед собой цели рассмотреть преимущества портативного компьютера перед классическим устройством под столом с монитором на три четверти стола. Намного важнее знать то, с чем могут столкнуться пользователи портативных компьютеров и как оптимально работать с ними.

Операционной системой в портативных компьютерах должна быть классическая Microsoft Windows XP Professional или Windows 2000. С портативными компьютерами под управлением других Windows-подобных систем типа Windows NT вы, вероятно, не встретитесь, потому что система Windows NT4.0 не располагает необходимыми функциями, а системы типа Windows 9x/ME не предназначены для корпоративной среды. Серверные операционные системы Windows 2000/2003 в портативных компьютерах скорее составляют исключение.

21.1. Автономные файлы

С тех пор, как у пользователей появилась возможность работать с документами в общих папках, расположенных на сервере, у них появилось и желание продолжать работу над ними и в отсутствие подключения к серверу. Пока утилит, облегчающих эту задачу, не существовало, пользователи были вынуждены придумывать собственные способы.

Один из таких способов — копирование необходимых файлов с сервера на локальный (портативный) компьютер, работа над ними у себя и копирование готовых документов обратно на сервер. Совместную работу над документом этот способ, понятно, сильно затрудняет: приходится искать способы согласования изменений, внесенных в один и тот же документ разными пользователями независимо друг от друга.

21.1.1. Портфель

Позднее в системах Windows появился инструмент **Портфель**, основной задачей которого было упростить процесс извлечения файлов с сервера и копирования их обратно после редактирования.

Этот инструмент отвечал своему времени и возможностям тогдашних технологий. Рядовым пользователям предлагалось применять **Портфель** самостоятельно, администратор помочь им не мог. В результате все знали, что в системе есть такой **Портфель**, приблизительно знали, для чего он служит, но практически никто (включая администраторов) его не использовал.

Для обеспечения совместимости (в интересах горстки пользователей, достаточно продвинутых, чтобы научиться с ним работать, и слишком консервативных, чтобы переключиться на другое средство) инструмент **Портфель** был включен в систему Windows XP Professional. Новым пользователям не обязательно учиться работать с ним, потому что начиная с Windows 2000 у них в распоряжении есть более мощное средство — **Автономные файлы**. Благодаря этому о **Портфеле** можно уже забыть.

21.1.2. Что такое Автономные файлы?

Эта функция предназначена для пользователей портативных компьютеров, которые работают над своими документами в дороге — разумеется, отключившись от файлового сервера. Одновременно она очень эффективно решает задачу синхронизации файлов, отредактированных «в дороге» (то есть вне сети), с соответствующими им файлами на сервере. Автономный файл представляет собой автоматически создаваемую локальную копию файла из общей папки на сервере.

По умолчанию функция **Автономные файлы** в клиентских операционных системах включена, но ее еще требуется настроить, причем в этом процессе должны участвовать как администратор, так и пользователь. Администратор отвечает за то, чтобы пользователю были доступны все документы, которые необходимы ему в дороге; пользователи отвечают за подготовку своих документов к отключению от сети и за правильную

синхронизацию при обратном подключении в случае конфликта между файлами в их компьютере и на сервере.

Функция **Автономные файлы** доступна в ОС семейства Windows 2000, в системах Windows XP Professional и Windows Server 2003 она расширена некоторыми интересными возможностями.

ОС этого семейства должна быть установлена на клиентской стороне. Возможность автономного доступа к файлам не зависит от того, какая операционная система стоит на компьютере, который открыл сетевой доступ к папке: там может быть как Windows 2000/XP/2003, так и одна из ранних версий — Windows 9x/ME или Windows NT 4.0.

Рассмотрим нашу сеть. Весьма вероятно, что функция **Автономные файлы** нужна только некоторым из наших пользователей.

1. Зарегистрируйтесь на PC001 как рядовой пользователь (например, Shop3).
2. Создайте новый документ в папке «Мои документы» (его название и содержание не имеют значения).
3. Завершите сеанс работы. Пока компьютер будет готовиться к выключению, обратите внимание на процесс синхронизации содержания папки «Мои документы».

Этот процесс в целом понятен. Для всех пользователей нашей сети при помощи групповых политик папка «Мои документы» перенаправлена на сервер, то есть в профиле пользователя хранится не содержание этой папки, а только путь к ней. В отличие от Windows 2000, в Windows XP Professional для всех перенаправленных папок по умолчанию настраивается режим **Автономные файлы.** Это значит, что, несмотря на перенаправление, новый файл в папке «Мои документы» создается на локальном жестком диске и только при выключении компьютера или завершении сеанса пользователя содержимое этой папки будет синхронизировано на сервер. В предыдущих версиях Windows новый файл в перенаправленной папке создавался прямо на сервере.

Таким образом, хоть мы ничего не настраивали специально, все пользователи, у которых папка «Мои документы» перенаправлена на сервер, незаметно для себя пользуются функцией **Автономные файлы.**

Разумеется, папка личных документов — не единственная из тех, к содержимому которых пользователям нужен автономный доступ в случае недоступности сети. Другие очевидные кандидаты — это папки подразделений в хранилище документов предприятия. Сейчас мы настроим автономный режим и для этих папок.

21.1.3. Включение автономного режима на рабочей станции

Только что мы убедились, что эта функция включена без каких-либо действий со стороны пользователя. Но вам, как администратору, необходимо знать, где именно она включается.

1. Зарегистрируйтесь на PC001 как администратор.
2. Запустите Проводник и выберите из строки меню команду **Сервис → Свойства папки**.
3. Перейдите на вкладку **Автономные файлы**. Автономный режим включается флажком **Использовать Автономные файлы.** Если вы видите этот флажок деактивированным, значит, вы зарегистрировались под именем рядового пользователя. Включить автономный режим имеет право только администратор. После этого этот режим будет доступен всем пользователям данного компьютера.

В клиентских операционных системах Windows XP Professional и Windows 2000 автономный режим разрешен сразу после установки. В серверных операционных системах (Windows 2000 Server и Windows Server 2003) он, наоборот, запрещен. В конце концов, кто будет путешествовать с сервером?

21.1.4. Настройка автономного режима

Требования пользователей к возможностям автономной работы различны. Одним необходим доступ ко всем файлам из папки, когда вздумается; другим достаточно иметь доступ только к некоторым файлам, но тоже всегда, а третьим достаточно доступа только к недавним документам (файлам, открывавшимся в последнее время). Это три разных варианта автономного режима, настройка которых входит в обязанности администратора сервера.

Автономные файлы сразу же после открытия помещаются в кэш — часть дискового пространства, доступ к которой возможен в любом состоянии соединения с сетью. Файлы, находящиеся в кэше, не имеют собственного значка, и автоматически удаляются из него, когда не хватает места на диске. В Windows Server 2003 имеются три варианта кэширования автономных файлов: автоматическое кэширование, ручное и запрет кэширования. Если кэширование для данной разделяемой папки запрещено, то пользователи вообще не смогут получить автономный доступ к ее файлам.

Автоматическое кэширование

В этом режиме в кэш помещается каждый открываемый пользователем файл из сетевой папки. Размер кэша для автономных файлов на клиент-

ском компьютере зависит от емкости диска. Значение по умолчанию — 10% от размера системного раздела. Отредактировать это значение можно на вкладке **Автономные файлы** окна свойств папок, и для этого нужны привилегии администратора.

Когда кэш заполнен, помещение в него новых файлов приводит к автоматическому удалению старых. Отсюда следует, что этот режим непригоден для файлов, автономный доступ к которым требуется всегда.

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Создайте папку `C:\Automatic`, а в ней текстовый файл. Откройте к этой папке сетевой доступ, оставив сетевое имя и права, предложенные по умолчанию.
3. Откройте окно свойств созданной папки и перейдите на вкладку **Доступ**. Нажмите кнопку **Кэширование** и установите переключатель в положение **В автономном режиме будут доступны все файлы и программы из этой папки**. Потом снимите флажок **Оптимизировать по производительности** и закройте диалоговое окно нажатием кнопки **ОК**.
4. Зарегистрируйтесь на PC001 как рядовой пользователь (например, Shop2).
5. Проверьте, включен ли режим **Автономные файлы**.
6. Откройте папку \\SRVR001\Automatic в Проводнике, после чего откройте имеющийся в ней текстовый файл.
7. В меню Проводника выберите команду **Сервис → Свойства папки**, перейдите на вкладку **Автономные файлы** и нажмите кнопку **Просмотр**. Откроется окно папки автономных файлов, в котором вы увидите свой текстовый файл.
8. Закройте текстовый файл и убедитесь, что в папке автономных файлов он остался.

Обычно на сервере хранятся приложения, нужные для работы многим пользователям (речь идет не о сетевом приложении, а об обычном, только запускаемом из общей папки). Тогда для папки с этим приложением выгодно будет настроить режим автоматического кэширования, оптимизированный по производительности. В этом случае при первом запуске такого приложения его исполняемый файл помещается в кэш, и следующий запуск происходит из кэша на локальном компьютере.

Таким образом снижается нагрузка на сеть и уменьшается время, затрачиваемое на второй и последующие запуски программы.

Ручное кэширование

В этом режиме в кэш помещаются только специально запрошенные пользователем файлы, то есть те, сохранение которых в памяти его интересует.

При этом файл помещается в кэш в ходе синхронизации. Как и в предыдущем случае, при нехватке места на диске файлы удаляются из кэша автоматически, но в данном режиме их можно удалять и вручную.

Чтобы автономные файлы были доступны пользователю, отключенному от сети, он должен перед отключением выполнить синхронизацию. Можно настроить и регулярную синхронизацию — по умолчанию раз в час.

Этот режим удобнее, чем предыдущий, поскольку при автоматическом кэшировании пользователю, чтобы обеспечить автономный доступ ко всей папке, нужно перед отключением от сети открыть все документы в ней.

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Откройте окно свойств папки `C:\Automatic` и перейдите на вкладку **Доступ**. Нажмите кнопку **Кэширование** и установите переключатель в положение **В автономном режиме будут доступны только файлы и программы, указанные пользователем**. Закройте диалоговое окно нажатием кнопки **ОК**.
3. Создайте в папке `C:\Automatic` другой текстовый файл.
4. Зарегистрируйтесь на PC001 как рядовой пользователь.
5. Проверьте, включен ли режим **Автономные файлы**, и перейдите в папку \\SRVR001\Automatic.
6. Откройте второй текстовый файл в этой папке.
7. В меню Проводника выберите команду **Сервис → Свойства папки**, перейдите на вкладку **Автономные файлы** и нажмите кнопку **Просмотр**. В папке автономных файлов вы не увидите второго текстового файла, потому что синхронизации еще не было.

Режим ручного кэширования предъявляет к пользователям самые высокие требования: они должны сами отмечать и синхронизировать нужные им файлы. Преимуществом этого режима является то, что заказанные файлы будут автономно доступны всегда.

Синхронизация файла

Синхронизация файла производится следующим образом:

1. Откройте папку \\SRVR001\Automatic.
2. Щелкните правой кнопкой мыши по текстовому файлу, который вы хотите синхронизировать, и из контекстного меню выберите команду **Сделать доступными автономно**. Запустится Мастер автономных файлов. Нажмите **Далее**.
3. В следующем окне установите флажок **Автоматически синхронизировать автономные файлы при входе в систему и при выходе из нее.** Нажмите **Далее.**
4. В следующем окне оставьте настройки по умолчанию и завершите работу Мастера нажатием кнопки **Готово**. Произойдет первая синхронизация файла.

5. Обратите внимание на изменение значка файла (автономные файлы, синхронизированные вручную, отличаются иконкой от остальных). В меню Проводника выберите команду **Сервис → Свойства папки**, перейдите на вкладку **Автономные файлы** и нажмите кнопку **Просмотр**. В папке автономных файлов вы увидите только что синхронизированный файл.

В табл. 21.1 приведено соответствие названий вышеперечисленных режимов в операционных системах Windows 2000/XP и Windows Server 2003.

Режимы кэширования *Таблица 21.1*

Windows 2000/XP	Windows Server 2003
Ручное кэширование	В автономном режиме будут доступны только файлы и программы, указанные пользователем (Only the files and programs that users specify will be available offline)
Автоматическое кэширование	В автономном режиме будут доступны все файлы и программы из этой папки (All files and programs that users open from the share will be automatically available offline)
Автоматическое кэширование программ и документов	То же + флажок **Оптимизировать по производительности**

21.1.5. Настройка синхронизации с помощью групповых политик

Методика настройки

Функция **Автономные файлы** — очень полезное свойство систем Windows 2000/XP/2003, и рекомендуется использовать ее везде, где это может потребоваться. Недостатком ее является необходимость настройки на стороне пользователя, предъявляющая определенные требования к его квалификации. Для опытного пользователя не составляет трудности вручную синхронизировать нужные ему файлы, а для всех остальных администратор домена может настроить автономный режим при помощи групповых политик.

Пользователям из разных подразделений нашего предприятия необходимо обеспечить автономный доступ к папке их подразделения в хранилище документов предприятия. Тогда они смогут работать с документами своего отдела на своих портативных компьютерах.

Политики управления автономными файлами находятся в обеих ветвях объекта групповой политики — и в **Конфигурации компьютера**, и в **Конфигурации пользователя**. В случае противоречия между ними приоритет имеют политики **Конфигурации компьютера.** Мы же будем настраивать **Конфигурацию пользователя,** поскольку требования к автономным файлам соответствуют организационной структуре нашего предприятия.

Рассмотрим настройку для отдела продаж.

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль **Active Directory — пользователи и компьютеры.**
2. Щелкните правой кнопкой мыши по контейнеру подразделения `Shop` и из контекстного меню выберите команду **Свойства**.
3. Перейдите на вкладку **Групповые политики** и создайте новый объект групповой политики. Дайте ему имя Offline Files (Shop).
4. В новом объекте раскройте ветвь **Конфигурация пользователя\Административные шаблоны управления\Сеть\Автономные файлы.**
5. В правом окне консоли вы увидите политики, относящиеся к автономным файлам. Включите из них следующие:
   - **Синхронизировать автономные файлы при входе в систему;**
   - **Синхронизация всех автономных файлов перед выходом из системы;**
   - **Синхронизировать автономные файлы перед приостановкой** (из списка **Действие** выберите «Полная»). Эта политика требует синхронизации перед переходом в спящий режим;
   - **Административно назначенные автономные файлы** (нажмите кнопку **Показать** и укажите путь `\\SRVR001\Библиотека\Продажи`).
6. Зарегистрируйтесь на PC001 как пользователь из отдела продаж (например, Shop1). В ходе регистрации произойдет синхронизация файлов из подпапки «Продажи» хранилища документов предприятия.
7. Запустите Проводник и в адресной строке введите путь `\\SRVR001\Библиотека\Продажи`. Обратите внимание на изменившиеся значки файлов в папке «Продажи».
8. Выберите из меню Проводника команду **Сервис → Свойства папки** и перейдите на вкладку **Автономные файлы**. Теперь настройки на этой вкладке изменить нельзя, потому что они регулируются групповыми политиками.

Повторите описанную процедуру для всех подразделений, кроме дирекции. Имейте в виду, что эта функция предназначена в основном для пользователей портативных компьютеров. Пользователи настольных компьютеров получают к ней доступ только тогда, когда недоступен файловый сервер.

Для пользователей из дирекции поступайте аналогичным образом, только в политике **Административно назначенные автономные файлы** укажите путь `\\SRVR001\Библиотека\`.

Хотя для каждого подразделения мы задали принудительную синхронизацию только одной папки, это не означает, что будет синхронизироваться только она. Каждый пользователь сможет самостоятельно добавить синхронизацию других папок или файлов. Групповая политика запрещает только отменять синхронизацию указанной папки.

Полная или частичная синхронизация?

В ходе работы с синхронизированными папками вы можете встретиться с понятиями «быстрая» и «полная» синхронизация. Что означают эти понятия?

При полной синхронизации происходит синхронизация всего содержимого папки. Это означает, что в автономном режиме вам всегда будут доступны текущие версии всех документов.

Быстрая синхронизация синхронизирует только файлы, которые присутствуют на обеих сторонах (в локальной папке и на сервере), причем с момента последней синхронизации их содержимое стало различным. Другие файлы (например, новые) остаются нетронутыми. Быстрая синхронизация происходит, когда на вкладке **Автономные файлы** сняты флажки **Синхронизировать**.

Поскольку применение только быстрой синхронизации может привести к рассогласованию между содержимым кэша и сетевой папки, необходимо время от времени выполнять полную синхронизацию. Для этого выберите из меню Проводника команду **Сервис → Синхронизировать**. Отобразится диалоговое окно со значками всех папок, для которых возможна синхронизация. Выберите нужную и нажмите кнопку **Синхронизация**.

Всегда полная синхронизация происходит, если на вкладке **Автономные файлы** окна **Свойства папки** установлены флажки **Синхронизировать**. Того же эффекта можно добиться, включив групповые политики **Синхронизировать автономные файлы при входе в систему** и **Синхронизация всех автономных файлов перед выходом из системы**.

21.1.6. Размещение автономных файлов

Размещение автономных файлов нельзя определить ни в одном диалоговом окне. Обычно эти файлы располагаются в скрытой папке `%Systemroot%\Client Side Caching`. Локальные копии документов находятся там в форме, непригодной для чтения, потому что вместе в ними хранится служебная информация.

Когда вы освобождаете место на диске, никогда не удаляйте файлы непосредственно из этой папки! Прямое вмешательство в ее содержимое может привести к потере данных на файловом сервере.

Удаление автономных файлов

Чтобы освободить место на диске, локальные копии сетевых файлов можно удалить. Для этого поступайте следующим образом:

1. Из меню Проводника выберите команду **Сервис → Свойства папки** и перейдите на вкладку **Автономные файлы**.
2. Нажмите кнопку **Удалить файлы.** Отобразится диалоговое окно **Подтверждение удаления файла.**
3. В списке папок оставьте отмеченными только те сетевые папки, копии файлов из которых вы собираетесь удалить. Если в нижней части окна вы поставите переключатель в положение **Удалить только временные автономные файлы**, то из кэша будут удалены только файлы, помещенные туда автоматически. Другое положение переключателя приведет к удалению всех файлов, в том числе синхронизированных вручную.

Иногда вышеописанным способом удалить локальные копии сетевых файлов не удается. В этом случае поможет переинициализация кэша автономных файлов: нажмите кнопку **Удалить файлы** при нажатой комбинации клавиш Ctrl+Shift, после чего перезагрузите компьютер.

Перемещение автономных файлов

Иногда оказывается необходимо переместить кэш автономных файлов на другой дисковый раздел того же компьютера (например, в целях оптимизации использования места на диске). Перемещение папки `%Systemroot%\Client Side Caching` здесь не поможет.

Следует воспользоваться утилитой Offline Files Cache Mover (**cachemov.exe**) из пакета Resource Kit для системы Windows 2000 Professional.

21.1.7. Шифрование автономных файлов

Режим автономного доступа чаще всего используется на портативных компьютерах — тех самых компьютерах, которые чаще всего воруют. Если вор доберется не только до личных документов хозяина компьютера, но и до документов предприятия, автоматически синхронизированных из сетевых папок, то ущерб может намного превзойти стоимость компьютера. Поэтому автономные файлы следует шифровать (эта возможность доступна только в Windows XP).

Чтобы включить шифрование файлов, помещаемых в кэш, установите флажок **Шифровать автономные файлы для защиты данных** на вкладке **Автономные файлы** окна **Свойства папки**.

Дальнейшую информацию о шифровании файлов вы найдете в 22 главе, посвященной безопасности сервера и сети.

21.1.8. Безопасность автономных файлов

Что, если системный раздел на компьютере пользователя отформатирован в файловой системе FAT32, не поддерживающей разрешений NTFS? Если такой пользователь синхронизирует файл, к которому он в сети предприятия имеет доступ только на чтение, отключится от сети и отредактирует его, то не сможет ли он таким образом изменить содержимое сетевого файла в процессе обратной синхронизации?

Нет, не сможет. В корпорации Microsoft об этом тоже подумали. Хоть локальная копия файла и будет помещена в раздел FAT32, пользователь не сможет редактировать этот файл: функция **Автономные файлы** умеет работать с исходными разрешениями, настроенными для сетевой папки.

21.1.9. Разрешение конфликтов

При редактировании автономных файлов может возникнуть конфликт между содержимым локальной копии и содержимым оригинального файла на файловом сервере. В таблице 21.2 перечислены возможные конфликты и способы их разрешения в процессе синхронизации.

Разрешение конфликтов при синхронизации файлов *Таблица 21.2*

Конфликт	Результат
Файл на сервере изменен другим пользователем	Синхронизация прерывается. Пользователю предоставляется возможность выбрать между своей версией файла, версией на сервере (своя в результате удаляется) или сохранить свою под другим именем
Файл на сервере удален другим пользователем	Синхронизация прерывается. Пользователю предоставляется возможность выбрать между своей версией (файл копируется на сервер) и версией на сервере (свой файл удаляется)
Администратор изменил права доступа к оригинальному файлу или папке на сервере	Если новые права доступа ограничивают пользователя сильнее, чем старые, то синхронизация прерывается, и пользователю показывают диалог авторизации, в котором он должен ввести регистрационные данные пользователя, имеющего необходимые полномочия. Если попытка авторизации не удалась, то синхронизации не произойдет

21.1.10. Групповые политики, управляющие автономными файлами

Мы уже назвали несколько политик, управляющих синхронизацией автономных файлов. Напоминаю, что эти политики находятся в обеих ветвях объекта групповой политики, причем в случае конфликта приоритет отдается политикам в ветви **Конфигурация компьютера.**

Перечислим еще несколько важных политик (табл. 21.3). В столбце Ветвь буква К обозначает ветвь **Конфигурация компьютера,** П — **Конфигурация пользователя.**

Политики, управляющие автономными файлами *Таблица 21.3*

Политика	Назначение	Ветвь
Разрешить или запретить использование автономных файлов	Соответствует флажку **Использовать автономные файлы**	К
Запретить пользовательскую настройку автономных файлов	Отключает вкладку **Автономные файлы** в окне **Свойства папки**	К, П
Размер кэша по умолчанию	Доля места на диске, умноженная на 10000 (например, 1000=10%)	К
Действия при отключении от сервера	Определяет, перейдет ли клиент в автономный режим, то есть будут ли копии сетевых файлов доступны локально	К, П
Нестандартные действия при отключении от сервера	Настройка действий при отключении от конкретных серверов	К, П
Удалить «Сделать доступными автономно»	Удаляет эту команду из контекстных меню файлов и папок	К, П
Запретить использование папки «Автономные файлы»	Отключает кнопку **Просмотр** на вкладке **Автономные файлы**	К, П
Некэшируемые файлы	Запрет кэширования файлов определенных типов. По умолчанию не кэшируются файлы с расширением SLM, MDB, LDB,MDW,MDE, PST и DB	К
При выходе из системы удалять локальную копию автономных файлов	Кэшированные файлы сохраняются только на протяжении сеанса пользователя. При выходе из системы файлы удаляются без синхронизации	К
Сделать подпапки всегда доступными в автономном режиме	Если делается доступной папка, то и все ее подпапки тоже	К
Шифровать кэш автономных файлов	Кэшируемые файлы автоматически шифруются	К
Запретить применение «Сделать доступными автономно» для этих файлов и папок	Запрещает делать доступными в автономном режиме конкретные файлы и папки	К, П
Настроить скорость медленного подключения	Когда сетевое подключение считается медленным (по умолчанию меньше 64 Кбит/с), при обнаружении сервера в сети автоматического подключения к нему не происходит с целью уменьшения трафика	К

21.2. Особенности применения групповых политик при подключении по медленной линии

В 17 главе мы настраивали групповые политики, управляющие рабочей средой на клиентских компьютерах и ограничивающие возможности пользователей по ее настройке. Пользователи портативных компьютеров обычно подключаются к сети предприятия по медленным линиям. Не

создаст ли в этом случае применение групповых политик избыточного трафика?

В 18 главе мы при помощи групповых политик установили в сети пакет MS Office, а в 20 главе установили пакеты обновления Service Pack. Будут ли приложения или пакеты обновления устанавливаться автоматически на портативные компьютеры? Ведь при такой установке по сети передается несколько мегабайт данных, что на медленной линии может занять несколько часов, а то и дней!

Вопросов по этому поводу достаточно, хорошо бы знать правильные ответы на них, чтобы при применении технологий IntelliMirror не было сюрпризов.

21.2.1. Что такое медленная линия?

Пользователи мобильных устройств отличаются от остальных пользователей домена прежде всего тем, что обычно они подключаются к сети нерегулярно и по медленной линии. Причем «недостаточная скорость связи» для каждой конкретной задачи своя: так, скорости линии может быть достаточно для повседневной работы пользователя, но совершенно недостаточно для установки по сети программного обеспечения.

Разработчики Windows 2000 позаботились о пользователях портативных компьютеров, разделив объект групповой политики на несколько частей. Если линия, по которой подключился пользователь, считается медленной, то ряд политик просто не применяется.

Пороговое значение, при скорости ниже которого линия считается медленной, настраивается через политики **Обнаружение медленных подключений для групповой политики** в ветвях **Административные шаблоны\Система\Групповая политика** в обеих частях объекта групповой политики. Значение, установленное в части **Конфигурация компьютера**, влияет на применение политик из этой части, а значение в части **Конфигурация пользователя** — независимо от него влияет на политики в соответствующей части.

Пороговое значение по умолчанию в обеих частях равно 500 Кбит/с.

На медленной линии по умолчанию применяются следующие политики:

- Настройка реестра (Административные шаблоны).
- Параметры безопасности.
- Политики восстановления EFS.
- Политики безопасности протокола IP.

Наоборот, по умолчанию не применяются:

- Установка программного обеспечения.
- Сценарии.
- Перенаправление папок.
- Дисковые квоты.
- Настройка Internet Explorer.

Если поведение на медленной линии по умолчанию вас не устраивает, вы можете разрешить или запретить применение других политик. Это делается установкой флажка **Разрешить обработку через медленное сетевое подключение**, активирующегося при включении соответствующей политики. Политики, для которых предусмотрена эта возможность, приведены в таблице 21.4.

Исключения из принципа обработки политик на медленных линиях *Таблица 21.4*

Политика	Результат
Обработка политики настройки Internet Explorer	Применяются политики, определенные в ветви **Конфигурация пользователя\Конфигурация Windows\ Настройка Internet Explorer**
Обработка политики установки программ	Применяются политики, определенные в ветвях **Конфигурация компьютера\ Конфигурация программ** и **Конфигурация пользователя\Конфигурация программ**
Обработка политики перенаправления папки	Применяются политики, определенные в ветви **Конфигурация пользователя\Конфигурация Windows\ Перенаправление папки**
Обработка политики сценариев	Запускаются сценарии, определенные в ветви **Конфигурация пользователя\ Конфигурация Windows\Сценарии**
Обработка политики дисковой квоты	Применяются политики, определенные в ветви **Конфигурация компьютера\Административные шаблоны\ Система\Дисковые квоты**

21.2.2. Как это повлияет на нашу сеть?

До сих пор мы подключали новые компьютеры к нашему домену только по локальной сети. Это подключение считалось быстрым, и все наши групповые политики применялись.

Пусть теперь одно из наших подразделений подключено к головному офису линией со скоростью 128 Кбит/с. В этом подразделении собственного контроллера домена нет. Если пользователь приехал в этот отдел со своим ноутбуком и подключился к сети предприятия оттуда, то контроллер домена обнаружит, что подключение происходит по медленной линии, и применит групповые политики так, что:

- Пользователю не будет предложено установить пакет MS Office (в главном меню не появятся соответствующие значки).

- Папка «Мои документы» не будет перенаправлена на сервер, а станет частью локального профиля.

Нужно ли изменить пороговое значение, ниже которого линия считается медленной (сейчас установлено 500 Кбит/с)? Нет. Рекомендуется никогда не устанавливать порог в точности равным номинальной пропускной способности линии: может случиться так, что в момент подключения компьютера скорость соединения окажется на самую чуточку больше, и контроллер домена мгновенно посчитает линию быстрой. В итоге он применит все политики, и по медленной линии пойдут мегабайты данных. Для нашей линии 128 Кбит/с значение 500 Кбит/с представляет вполне достаточный запас прочности.

21.2.3. Что произойдет с профилями пользователей?

Порог определения медленной линии используется также для определения, можно ли применять перемещаемые профили. Когда пользователь с перемещаемым профилем впервые регистрируется на некотором компьютере, весь его профиль копируется с сервера. Если компьютер подключен по медленной линии, а профиль велик, то процесс копирования может продолжаться несколько часов. Поэтому на медленных линиях следует отключить применение перемещаемых профилей.

Сделать это можно через политику **Таймаут для профилей пользователей для медленных сетевых подключений** в ветви **Конфигурация компьютера\Административные шаблоны\Система\Профили пользователей.**

В окне настройки этой политики можно указать не только пороговое значение скорости, но и время отклика. Это время применяется для серверов, работающих не по протоколу TCP/IP.

Если пользователь с перемещаемым профилем впервые регистрируется на компьютере, где применение перемещаемых профилей запрещено, то для него создается локальный профиль, включающий локальную же папку «Мои документы». К своим документам на сервере он сможет получить доступ, только указав UNC-путь к «бывшей своей» сетевой папке, то есть тот путь, который он видел в окне свойств папки «Мои документы» при подключении по быстрой линии.

Во избежание такой неприятности рекомендуется создать локальную копию перемещаемого профиля, то есть впервые зарегистрироваться на своем портативном компьютере тогда, когда он подключен по локальной сети. Тогда же следует и установить по сети все нужные приложения. Не забудьте только отключить политику **Удалять кэшированные копии перемещаемых профилей** в ветви **Конфигурация компьютера\Административные шаблоны\Система\Профили пользователей.** Если эта политика

включена, то локальная копия будет удалена при завершении сеанса работы, и при подключении по медленной линии пользователь останется без профиля.

При первой регистрации пользователя его регистрационные данные также помещаются в локальный кэш. Это обеспечивает возможность в дальнейшем регистрироваться и тогда, когда контроллер домена недоступен.

21.3. Настройка портативного компьютера в нашей сети

Допустим, что PC002 — это ноутбук. Его учетная запись находится в контейнере **Компьютеры**. Кроме политик, общих для всех компьютеров домена, мы собираемся применить к нему политики, специфичные для портативных компьютеров, поэтому переместим его учетную запись в контейнер **Портативные**, который создадим внутри контейнера **Компьютеры**.

На уровне организационной единицы **Портативные** создайте новый объект групповой политики и дайте ему имя, к примеру, Portable Computers. В этом объекте мы будем настраивать только политики в разделе **Конфигурация компьютера**, поскольку нам безразлично, кто именно из пользователей будет за данным компьютером работать удаленно.

Включите следующие политики:

В ветви **Административные шаблоны\Сеть\Автономные файлы**:

- Разрешить или запретить использование автономных файлов;
- Шифровать кэш автономных файлов.

В ветви **Административные шаблоны\Система\Группповая политика:**

- **Обработка политики перенаправления папки** (включите флажок **Разрешить обработку через медленное сетевое подключение**).

Отключите следующую политику:

Административные шаблоны\Система\Профили пользователей\Удалять кэшированные копии перемещаемых профилей.

21.4. Итоги

С точки зрения управления доменом группа пользователей портативных компьютеров является особой и требует отдельного администрирования.

Основная особенность ее заключается в том, что эти пользователи подключены к сети не постоянно и чаще всего по медленным линиям.

Пользователю, подключающемуся у сети предприятия издалека, тоже нужен доступ к документам в общих папках на файловом сервере. Поскольку открывать эти папки вручную не всегда выгодно и возможно, следует настроить режим автономного доступа к этим папкам, автоматически синхронизирующий состояние сетевых файлов с их локальными копиями при подключении и отключении от сети. Функция **Автономные файлы** умеет сохранять разрешения NTFS, даже если кэширование производится в раздел FAT. Дополнительно защитить автономные файлы можно шифрованием кэша.

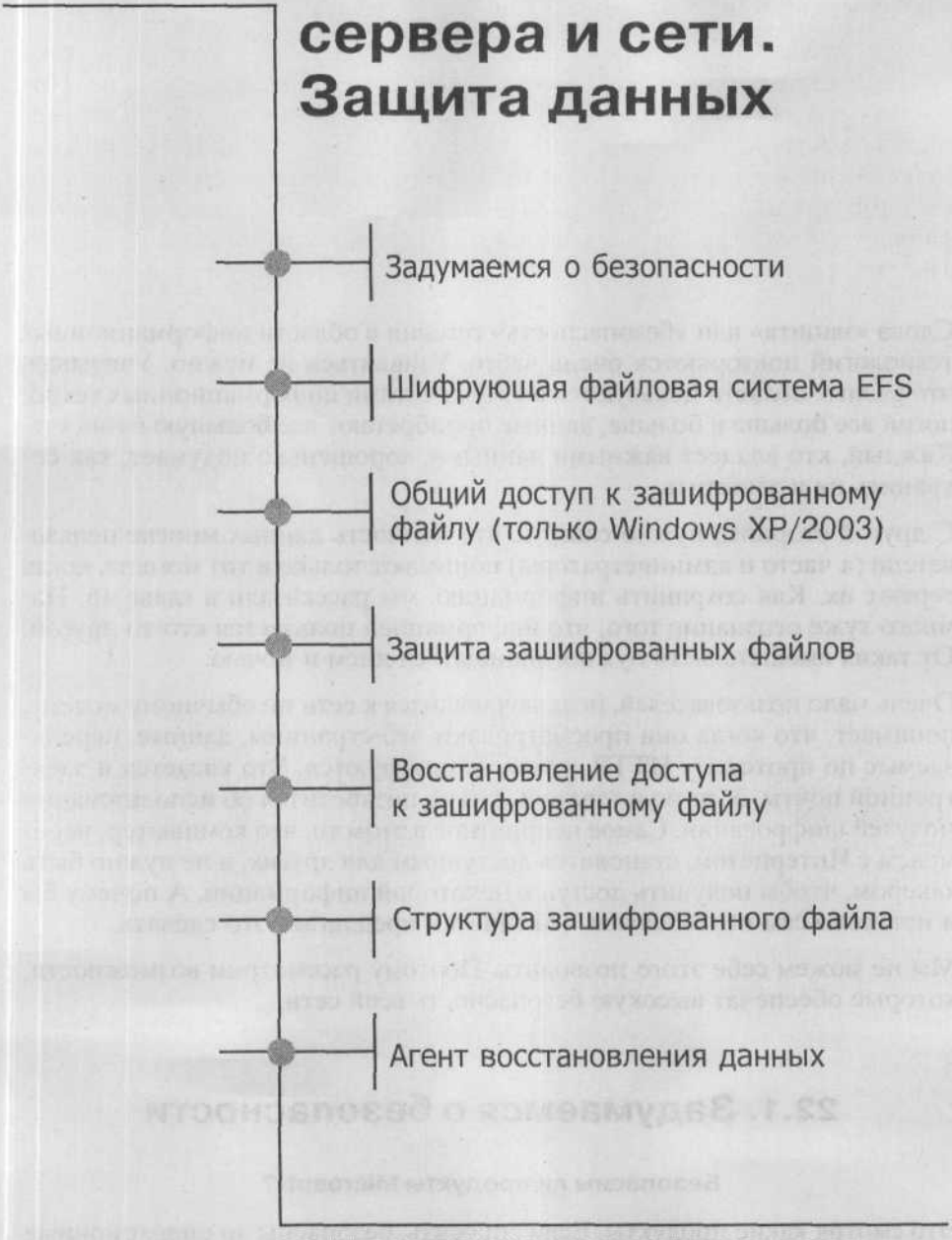
К компьютерам, подключенным к сети по линии, считающейся медленной, во избежание лишнего трафика применяются не все групповые политики. По умолчанию пороговым значением скорости соединения является 500 Кбит/с. В частности, по медленной линии отменяется автоматическая установка программного обеспечения и применение перемещаемого профиля. Чтобы пользователь портативного компьютера получил привычную рабочую среду (локальную копию профиля), он должен впервые зарегистрироваться на этом компьютере тогда, когда тот подключен к сети по быстрой линии.

Состояние сети

Мы настроили автономный доступ к общим папкам. Теперь каждый пользователь сможет самостоятельно синхронизировать нужные ему сетевые файлы. Кроме того, для каждого подразделения мы настроили принудительную синхронизацию соответствующей подпапки в хранилище документов предприятия — на тот случай, если пользователи синхронизировать файлы не умеют.

Все портативные компьютеры мы настроили для удаленной работы по медленным линиям, объединив их в отдельную организационную единицу внутри контейнера Компьютеры и создав для нее отдельный объект групповой политики.

Глава 22 Безопасность сервера и сети. Защита данных



Слова «защита» или «безопасность» сегодня в области информационных технологий повторяются очень часто. Удивляться не нужно. Учитывая, что разные области пользуются возможностями информационных технологий все больше и больше, данные приобретают все большую ценность. Каждый, кто владеет важными данными, хорошенько подумает, как сохранить их и защитить.

С другой стороны, нужно сказать, что ценность данных многие пользователи (а часто и администраторы) понимают только в тот момент, когда теряют их. Как сохранить информацию, мы рассказали в главе 16. Намного хуже осознание того, что информацией пользуется кто-то другой. От таких вмешательств нужно защищаться днем и ночью.

Очень мало пользователей, подключающихся к сети по обычному модему, понимает, что когда они просматривают веб-страницы, данные, передаваемые по протоколу HTTP, никак не шифруются. Это касается и электронной почты, если пользователь сам не позаботится об использовании модулей шифрования. Самое неприятное в этом то, что компьютер, через модем с Интернетом, становится доступным для других, и не нужно быть хакером, чтобы получить доступ к некоторой информации. А почему бы и нет, если сам пользователь фактически предлагает это сделать.

Мы не можем себе этого позволить. Поэтому рассмотрим возможности, которые обеспечат высокую безопасность всей сети.

22.1. Задумаемся о безопасности

Безопасны ли продукты Microsoft?

Это смотря какие продукты. Если спросить, безопасны ли операционные системы Windows 2000/XP/2003 компании Microsoft, то ответ будет — да, эти продукты высоко надежны. Но при этом нужно добавить, что не в своем исходном состоянии.

Представьте ситуацию, что вам нужно передать посредством электронной почты заказчику данные (имя и пароль) для подключения к торговой системе. Электронная почта в изначальном состоянии не защищена, и данные, отправленные с ее помощью, может прочитать любой администратор, имеющий доступ к серверу электронной почты.

Так поступать не рекомендуется. Нужно представить себе, что может случиться в том случае, если отправленные данные получит совсем другой человек. Речь идет о потенциальном риске, и необходимо хорошо продумать, допустим ли он для вас.

Какие же еще есть возможности передачи информации? Несколько безопаснее будет отправление имени и пароля в двух отдельных сообщениях, или, например, отправление пароля другим способом (по факсу). Еще безопаснее будет зашифровать сообщения электронной почты.

Как видите, возможностей предостаточно. Если вы решите зашифровать электронное письмо, вам нужно будет отправить ключ шифрования получателю. Если вы собираетесь защитить свои данные, то не думайте, что вам это удастся на 100%. Всегда найдется способ получить доступ к информации. Иногда может получиться, что нежеланным «гостем» станет ваш коллега — администратор, у которого есть такой же доступ ко всему, как и у вас. О максимальной защите информации можно говорить только тогда, когда риск сведен к минимуму.

Вернемся к защищенности операционных систем компании Microsoft. В свое время системы Windows 2000 появились на рынке как совершенно новая разработка с широкими возможностями. И многие элементы, о которых пользователи даже и не подозревают, устанавливаются автоматически. В результате на каждом сервере с системой Windows 2000 Server устанавливался, например, веб-сервер. А если через некоторое время в нем обнаруживалась ошибка, то возникала угроза безопасности системы.

Система Windows Server 2003 в этом плане радикально отличается от Windows Server 2000.

Еще до ее появления на рынке компания Microsoft выступила с лозунгом "Trustworthy Computing" («надежный компьютер»). Результатом явилось то, что после инсталляции системы не работает ничего. Все, что администратору необходимо, он должен настроить сам, например, запретить при открытии сетевого доступа к папке предоставлять по умолчанию разрешение «Полный доступ» группе «Все».

Вместе с тем создатели системы Windows Server 2003 подумали о множестве администраторов и сделали настройки безопасности по умолчанию такими, чтобы они подходили всем. Это привело к тому, что настройки по умолчанию не подходят никому. Ведь кто-то может использовать систе-

му Windows Server 2003 как файловый сервер, другие — как контроллер домена. И ясно, что в каждом случае будет необходима разная степень защиты и параметры безопасности будет необходимо настроить именно под свои требования.

Итак, операционные системы, с которыми мы работаем в этой книге, теоретически безопасны, но чтобы они стали таковыми на практике, нужно предпринять некоторые действия.

От кого нужно защищаться?

Не нужно думать, что сеть может подвергнуться нападению только извне. Обеспечение безопасности на уровне пользователей сети является также обязательным. Многие, отвечающие за безопасность, могут заметить, что это не нужно, так как:

- Все пользователи подписали соглашение о том, как будут использовать компьютер, и их противоправные действия будут поводом для увольнения. Поэтому каждый думает о том, что он делает.
- Серверы защищены, поскольку на них установлены все выпущенные обновления Service Pack.

Нужно, чтобы администраторы понимали следующее:

- В любой момент в операционной системе может быть обнаружена «дырка», и любознательный пользователь может ею воспользоваться. Необязательно злонамеренно — просто по незнанию он может причинить вред системе. Обновление Service Pack латает эти дыры, но само по себе не может обеспечить защиту.
- Далеко не всегда пользователи увольняются за «покушение» на сервер. Может случиться, что работника увольняют, как он считает, незаслуженно, и перед уходом он может так «отомстить».

Ясно, что самая большая угроза для серверов — это пользователи из Интернета. Но нельзя забывать и про внутренних пользователей.

Защита данных

Данные, которые находятся в компьютере, можно разделить на более или менее важные. Как уже говорилось, часто ценность данных пользователь определяет в тот момент, когда они пропадут. Еще большую ценность приобретают те данные, которые не пропали, а попали в руки того, кто не должен был иметь к ним доступ.

Системы Windows 2000/XP/2003 относятся к группе защищенных систем. Это означает, что эти системы способны защитить данные в компьютере так, чтобы к ним имел доступ только пользователь-владелец. Однако для этого нужно кое-что сделать.

Файловая система и способы защиты

При инсталляции сервера (глава 1) и компьютеров пользователей (глава 2) мы без долгих размышлений выбрали файловую систему NTFS. Только эта система способна обеспечить безопасность данных, однако для этого необходимы определенные действия.

Если решите форматировать жесткий диск в другой файловой системе (FAT или FAT32), его можно будет позже конвертировать в систему NTFS. Однако назад вернуться без потери данных уже нельзя.

Единственной причиной для форматирования дисков в другой файловой системе, не NTFS, может быть наличие на компьютере альтернативной операционной системы (так называемая dual-boot или multi-boot конфигурация, система с двойной загрузкой), не поддерживающей NTFS.

Основное преимущество NTFS — это возможность настройки разрешений на доступ к ресурсам. Но этого не всегда достаточно. Представьте, что ваши данные украли вместе с компьютером. Не зная вашего имени и пароля, злоумышленник не сможет зарегистрироваться, чтобы прочитать эти данные, но никто не мешает ему извлечь ваш жесткий диск и переставить его на свой компьютер, где он получит доступ ко всем вашим файлам.

То же самое произойдет, если вы оставите включенный компьютер без присмотра и злоумышленник будет иметь доступ на уровне вашей учетной записи.

Поскольку стопроцентно гарантировать физическую недоступность ваших данных для злоумышленника невозможно, следует найти способ сделать так, чтобы он не смог их прочитать. За решением, к счастью, далеко ходить не нужно — частью операционной системы, точнее файловой системы NTFS, является система шифрования.

22.2. Шифрующая файловая система EFS

Шифрующая файловая система (Encrypting File System, EFS) является одним из свойств системы NTFS в ОС Windows, начиная с Windows 2000. Шифровать можно отдельные файлы или целые папки. Если зашифровать всю папку, то, естественно, зашифруются и все содержащиеся в ней файлы.

С точки зрения пользователей процесс шифрования происходит быстро и просто. Подробностей процесса (как и когда происходит шифровка и расшифровка файлов) им знать не нужно. Боле того, сам процесс шифрования остается для них незаметным: они даже не увидят разницы между

открытием в приложении зашифрованного файла и нешифрованного. К сожалению, и здесь есть свои подводные камни. Проще говоря — как быстро и без проблем можно зашифровать файл, так же быстро и легко можно лишиться возможности его декодировать.

Было бы замечательно, если бы пользователи знали принципы шифрования, используемые системой EFS, но их квалификация не всегда позволяет на это надеяться. Поэтому проще предположить, что пользователи этого знать не будут (и не нужно их винить в этом), а к неожиданностям придется готовиться администратору.

Для начала немного теории.

22.2.1. Принципы шифрования

Целью шифрования является перенос важного документа адресату в той форме, которую он будет способен расшифровать. Исходный файл необходимо зашифровать так, чтобы расшифровать его смог только адресат. Для этого у адресата должен иметься ключ.

На практике можно встретиться с двумя способами шифрования — симметричным и асимметричным. Различаются эти способы использованием ключа.

Симметричное шифрование

Этот способ характеризуется тем, что для шифровки и дешифровки данных служит один и тот же (симметричный) ключ. Проблема заключается в том, как передать этот ключ адресату. Эта передача должна быть безопасной, так как кто угодно, получивший ключ в свое распоряжение, получит и доступ к зашифрованным файлам.

Решите вопрос безопасной передачи ключа шифра. Телефонный разговор? Электронное письмо? Шифрование самого ключа? Вряд ли: все эти способы известны и не дают необходимой гарантии безопасности.

С другой стороны, если мы решили вопрос передачи ключа шифрования, у симметричной шифровки по простоте, быстроте и нагрузке на компьютер нет конкурентов.

Подведем итог — симметричная шифровка проста и быстра; единственной проблемой остается передача ключа шифрования.

Асимметричное шифрование

Это способ шифрования при помощи пары ключей, один из которых служит только для шифровки данных, а другой только для расшифровки.

Ключи в этой паре связаны математическим алгоритмом так, что ключ от другой пары для расшифровки непригоден.

Названия этих ключей подсказывают способ обращения с ними. Один из ключей называется *закрытым*, то есть его нужно хранить как зеницу ока. Другой называется *открытым*, и его можно сообщать кому угодно.

Процесс асимметричного шифрования сложнее симметричного, так как здесь фигурирует больше ключей. Кроме того, требуется больше места на жестком диске и весь процесс занимает больше времени.

Комбинированное шифрование

Сравнивая два способа шифрования, сделаем вывод, что лучше всего использовать симметричную шифровку, которая проще и быстрее, но нужно придумать механизм для передачи ключа. И именно для этой цели будем использовать асимметричную шифровку. Порядок действий будет следующим:

Как отправитель важного документа придумайте симметричный ключ, с помощью которого будете в дальнейшем шифровать документ (например, `ABC123`).

Затем попросите адресата, чтобы отправил вам открытый ключ. Вы можете его требовать, и партнеру нечего бояться.

Открытый ключ адресата используйте для шифрования ключа, который вы перед этим придумали (симметричного). Результат отправьте адресату, например, по электронной почте (допустим, после шифровки получилось `XYZ567`).

Этот результат сможет правильно расшифровать только тот, кто владеет вторым из пары ключей. Понятно, что это может быть только адресат, который передал вам свой открытый ключ. Используя закрытый ключ, он откроет полученное сообщение и получит исходный ключ `ABC123`.

Приведенный способ представляет собой безопасную передачу ключа для симметричного шифрования. Затем, когда обе стороны владеют симметричным ключом, они могут перейти на симметричную шифровку и обмениваться зашифрованными документами.

Теории пока достаточно, перейдем к практике. Комбинация симметричной и асимметричной шифровки используется и в системе EFS. Очень важно понять, что возможность расшифровывать файл связана напрямую не с учетной записью пользователя, а только с наличием необходимого ключа.

Эта технология, впервые представленная в системе Windows 2000, уже несколько лет находится на рынке, и уже можно встретить жертв ее не-

осторожного применения. Представим, что на диске **D:** была применена функция шифрования файлов. В один прекрасный момент пришлось переустановить операционную систему, установленную на диске **C:**. В итоге доступ к содержимому зашифрованных файлов тотчас был потерян.

Чтобы не попасть в такую неприятную ситуацию или, точнее, чтобы в такую ситуацию не попали ваши пользователи, нужно знать, как работает ключ шифрования в системах Windows 2000 и Windows XP Professional и какие есть возможности возобновления доступа к шифрованным файлам.

Примечание.

Шифрующая файловая система EFS не поддерживается в версии Windows XP Home Edition.

22.2.3. Шифрование на практике, или первая встреча с EFS

Согласно вышеприведенной информации, система EFS использует комбинацию двух типов шифрования — симметричную и асимметричную. Таким образом, ясно, что будет необходимо иметь несколько ключей. Заботиться нужно только об асимметричных ключах: ключ для симметричной шифровки генерируется операционной системой автоматически и пользователю (администратору) его вообще знать не нужно.

Так как возможности шифрования файловой системы в системе Windows XP Professional расширены по сравнению Windows 2000, некоторые из приведенных ниже сведений действительны в обеих операционных системах, а другие верны только в Windows XP Professional.

22.2.4. Ключи и сертификаты

В связи с использованием пары ключей для асимметричной шифровки можно столкнуться с понятием *сертификат*. Что это такое? В примере выше были описаны действия по обмену ключами при помощи асимметричного шифрования. Все начинается с того, что адресат передает отправителю свой открытый ключ.

На это надо обратить внимание. Учитывая, что партнеры хотят обменяться важной информацией (используя ключ, которым потом можно будет расшифровывать ваши файлы), нужно быть уверенным, что этот ключ вы будете шифровать открытым ключом, которым владеет «нужный» партнер. Поэтому нужно быть уверенным в том, от кого пришло это сообщение.

Каждый, кто рассчитывает на ваше доверие, не будет посылать вам свой открытый ключ просто так, а подпишет его в сертифицирующей

организации (Certification authority, CA). Эта организация отвечает за то, что подписанный открытый ключ действительно принадлежит тому, чьи данные в этом ключе записаны.

Если вы подписываете свой открытый ключ в сертифицирующей организации, вы получаете *Сертификат*. Сертификат — это не что иное, как подписанный открытый ключ.

Всю эту область, которая занимается асимметричной шифровкой и сертификатами, называют *инфраструктурой открытого ключа* (Public Key Infrastructure, PKI).

В дополнение к основной информации и для упрощения представления о шифровании EFS нужно сказать, что получатель и отправитель в данном случае меняются ролями.

22.2.5. Первый зашифрованный файл

Методика шифрования

Чтобы не заполнять место лишними ключами и сертификатами, используем для первой шифровки экспериментальную учетную запись пользователя, которую создадим специально для этой цели:

1. Зарегистрируйтесь на PC001 как администратор и запустите оснастку **Active Directory — пользователи и компьютеры.**
2. В контейнере **Users** создайте экспериментальную учетную запись с именем `efsuser`.
3. Зарегистрируйтесь на компьютере как пользователь `efsuser`.
4. Запустите Проводник и создайте папку `C:\EFSUSER`. В ней создайте новый текстовый файл. Запишите в него несколько слов и сохраните файл.
5. Откройте окно свойств этого файла и перейдите на вкладку **Общие**.
6. Нажмите кнопку **Дополнительно** и затем в диалоговом окне **Дополнительные атрибуты** установите флажок **Шифровать содержимое для защиты данных**.
7. Закройте диалоговые окна нажатием кнопки **OK**.
8. В диалоговом окне **Предупреждение при шифровании** выделите поле **Зашифровать только файл** и нажмите **OK**.

Теперь текстовый файл зашифрован. В этом вам легко убедиться как администратору компьютера:

1. Зарегистрируйтесь на компьютере PC001 как администратор.
2. Запустите Проводник и перейдите в папку `C:\EFSUSER`. Попытайтесь открыть зашифрованный файл (в Windows XP он отображается

зеленым цветом, в Windows 2000 цветного выделения нет). Вы увидите сообщение о том, что доступ к файлу закрыт.

Таким образом, пользователь `efsuser` зашифровал собственный файл, скрыв его содержимое даже от администратора, по идее имеющего доступ ко всему. Если бы при шифровке отображалась вся информация (которую ему знать не обязательно), он бы увидел, что создалась пара ключей, которые принимают участие в шифровке и расшифровке. Открытый ключ был подписан, и ключи стали частью профиля пользователя.

Теперь пользователь абсолютно спокоен, потому что уверен, что никто не откроет его файл. Администратор не был бы так спокоен, так как весь процесс шифрования еще недостаточно надежен. Мы видели, что даже администратор не сможет прочитать файл, а что скажет пользователь `efsuser`, который зашифровал файл и теперь не может открыть? Можно ли ему как-то помочь? Далее в этой главе мы расскажем о том, какие изменения произошли в системе и что нужно сделать для обеспечения безопасности последующего открытия зашифрованных файлов.

Проверка существования ключей пользователя

Создание необходимых ключей для пользователя `efsuser` прошло незаметно на фоне процесса шифрования. Это происходит только в том случае, когда еще не существует ни один ключ шифрования. Когда пользователь захочет зашифровать очередной файл, для этого будет использован уже готовый ключ. Где сохранен этот ключ и как можно его просмотреть, мы сейчас узнаем.

1. Зарегистрируйтесь на компьютере PC001 как пользователь `efsuser`.
2. Запустите пустую консоль MMC.
3. Выполните команду **Консоль → Добавить или удалить оснастку** и добавьте оснастку **Сертификаты**.
4. Разверните ветвь **Сертификаты — текущий пользователь\Личные\Сертификаты** и в правом окне консоли щелкните по сертификату **efsuser.**

В сертификате можно найти много полезной информации. На вкладке **Состав** узнайте, когда именно сертификат был создан (поле **Действителен с**). Дата и время создания сертификата должны соответствовать времени шифрования файла. Затем убедитесь, что сертификат действителен в течение 100 лет, и можете проверить открытый ключ.

Кто создал сертификат? Иными словами, кто подписал открытый ключ? Это вы увидите на вкладке **Путь сертификации.**

Здесь приведена единственная запись — `efsuser` — более того, обведена красным цветом. Речь идет о нестандартных ситуациях, когда

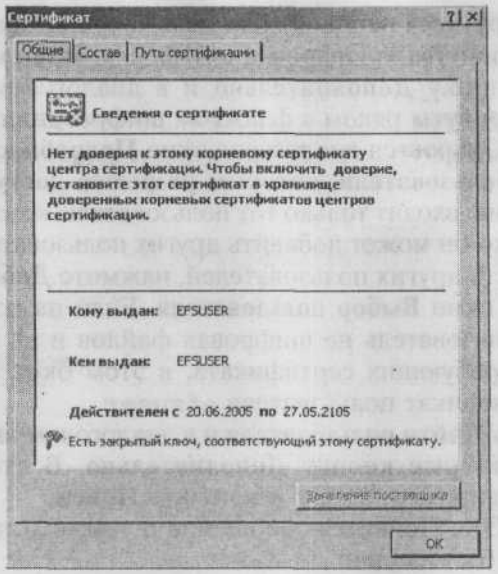


Рис. 22.1. *Сертификат пользователя efsuser*

сертификат подписан «сам собой». Выделение красным цветом означает, что сертификат не заслуживает доверия, так как его не подписала ни одна сертификационная служба. Так ведут себя сертификаты корневых сертификационных служб и сертификаты, созданные для особых целей (например, для файловой системы EFS). Остальные сертификаты бывают подписаны сертификационными службами — к этому мы еще придем.

На вкладке **Общие** в нижней части указано «Есть закрытый ключ, соответствующий этому сертификату». Это означает, что где-то на компьютере хранится закрытый ключ пользователя `efsuser`, который составляет пару с его открытым ключом. «Где-то» в данном случае означает «в профиле пользователя». Это важно, так как при попытке пользователя `efsuser` открыть зашифрованный файл он тут же откроется.

22.3. Общий доступ к зашифрованному файлу (только Windows XP/2003)

Обычно доступ к файлу имеет только пользователь, который его зашифровал. Однако система Windows XP Professional предлагает еще большие возможности — сделать зашифрованный файл общим для доступа других пользователей. В Windows 2000 это невозможно.

1. Зарегистрируйтесь на PC001 как пользователь `efsuser`.
2. Откройте свойства зашифрованного файла. Затем на вкладке **Общие** нажмите кнопку **Дополнительно** и в диалоговом окне **Дополнительные атрибуты** рядом с флажком шифрования нажмите кнопку **Подробно**. Откроется диалоговое окно **Подробности шифрования.**
3. В список **Пользователи, которым разрешен доступ к этому файлу** по умолчанию входит только тот пользователь, который зашифровал файл. Только он может добавить других пользователей. Если вы хотите добавить других пользователей, нажмите **Добавить.** Откроется диалоговое окно **Выбор пользователя.** Если на компьютере PC001 ни один пользователь не шифровал файлов и не выполнял других действий, требующих сертификата, в этом окне будет отображен только сертификат пользователя `efsuser`.
4. Нажмите на **Найти пользователя** и в диалоговом окне **Выбор: Пользователь** нажмите кнопку **Дополнительно**. В открывшемся окне наберите, например, `Shop1` и нажмите **Поиск.**
5. Щелкните **ОК.** Появится сообщение о том, что необходимый сертификат не был найден.

Оказывается, разделить зашифрованный файл возможно только с тем пользователем, у которого есть сертификат. Чтобы другой пользователь получил свой сертификат, ему нужно зашифровать какой-нибудь файл на компьютере PC001.

Требовать от другого пользователя, чтобы он зашифровал что попало для того, чтобы мы смогли открыть ему доступ к действительно важным зашифрованным данным, достаточно неудобно. Если бы можно было иметь открытый ключ (сертификат) другого пользователя независимо от того, шифровал ли он что-нибудь на данном компьютере, то вы, как владелец зашифрованного файла, не были бы связаны действиями других пользователей и могли бы организовать общий доступ к этому файлу единолично.

Это возможно, но в нашей сети мы настраивать такую возможность не будем, потому что для этого нужно установить сертификационную службу на компьютер под управлением ОС Windows Server 2003 Enterprise Edition, которой у нас в сети нет.

Однако кое-что мы можем сделать. Сертификационная служба нашей операционной системы, Windows Server 2003 Standard Edition, автоматически публикует все открытые ключи в домене Active Directory. То есть пользователь сможет передать свой зашифрованный файл другому пользователю, если тот уже шифровал что-либо на любом компьютере домена.

Типы сертификационных служб в системе Windows 2000/2003

Сертификационные службы в серверных операционных системах Windows 2000/2003 можно разделить на две группы:

- **Сертификационная служба для больших сетей.** Эта сертификационная служба (в выпуске Enterprise CA) предназначена для пользователей домена. Каждая сертификационная служба перед тем, как подписать открытый ключ, проверяет пользователя. Так как сертификационной службе больших сетей для проверки пользователя достаточно наличия его доменной учетной записи, эта служба создает сертификат автоматически. Для наших целей — автоматического создания сертификата при попытке шифрования — этот тип сертификационной службы является не просто оптимальным, а единственно возможным.
- **Самостоятельная сертификационная служба.** Эта сертификационная служба способна создать сертификат (подписать открытый ключ) как пользователям домена, так и пользователям, не входящим в домен. В этом случае нет возможности автоматически создавать сертификаты, потому что пользователь должен подтвердить свою личность вручную. Это могут сделать только авторизованные пользователи, которые и несут ответственность за достоверность данных, указанных в сертификате. Для нашей цели этот тип службы непригоден, но на практике он используется чаще всего. Именно таким способом рядовой пользователь получает так называемый самоподписанный сертификат.

Сертификационные службы можно объединять в иерархические структуры, и на практике с этим можно встретиться. Этому соответствуют атрибуты сертификационных служб — корневая и подчиненная. Если вы хотите установить подчиненную сертификационную службу, нужно «приобрести» сертификат, подписанный корневой службой. Корневая служба подпишет открытый ключ сама — иначе это не будет корневая служба.

Итог — нашим требованиям подходит ***Корневой сертификат для большой сети.***

Установка сертификационной службы

Установка сертификационной службы может существенно повлиять на работу сети, тем более, если речь идет о корневой службе. Ее настройка, которая происходит во время установки, так же повлияет на все имеющиеся сертификаты. Если вы не уверены в значении отдельных настроек, лучше прервать процесс установки и посмотреть описание.

1. Зарегистрируйтесь на компьютере SRVR001 как администратор.
2. Запустите апплет **Установка и удаление программ** и выберите задачу **Установка компонентов Windows.**

3. В диалоговом окне **Установка компонентов Windows** отметьте флажком **Сертификационная служба (Certificate Services).** Отобразится сообщение о том, что после установки этого компонента нельзя будет изменить имя компьютера и его членство в домене. Нажмите **Да** и затем **Далее.**
4. В диалоговом окне **Тип ЦС** выделите окошко **Корневой ЦС предприятия** и нажмите **Далее.**
5. В диалоговом окне **Сведения о центре сертификации** в поле **Общее имя для этого ЦС** введите имя сертификационного центра (например, **Study CA**). В названии не используйте символов кириллицы, иначе вы можете вызвать несовместимость сертификатов с некоторыми (старыми) приложениями. В части **Срок действия** задайте значение 5 лет. Продолжите нажатием кнопки **Далее.** Будет создана пара ключей для этой службы.
6. В диалоговом окне **Параметры базы данных сертификатов** сохраните исходные пути к базе данных сертификатов и протоколу и нажмите **Далее.** Начнется установка сертификационной службы, в ходе которой у вас потребуют вставить инсталляционный компакт-диск Windows Server 2003.
7. Завершите работу Мастера установки нажатием кнопки **Готово.** Компьютер не требует перезагрузки.

Примечание.

Получить сертификат у сертификационной службы можно также с помощью веб-браузера. В таком случае на компьютере должен быть установлен сервер IIS. Если его нет (как у нас сейчас), во время установки сертификационной службы появится предупреждающее сообщение.

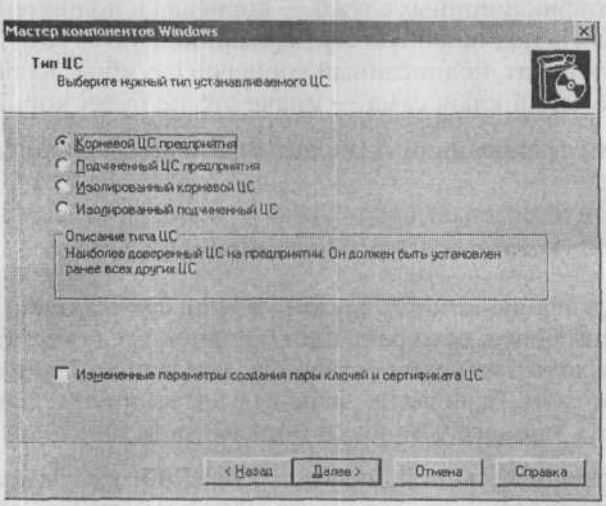


Рис. 22.2. *Выбор типа сертификационной службы*

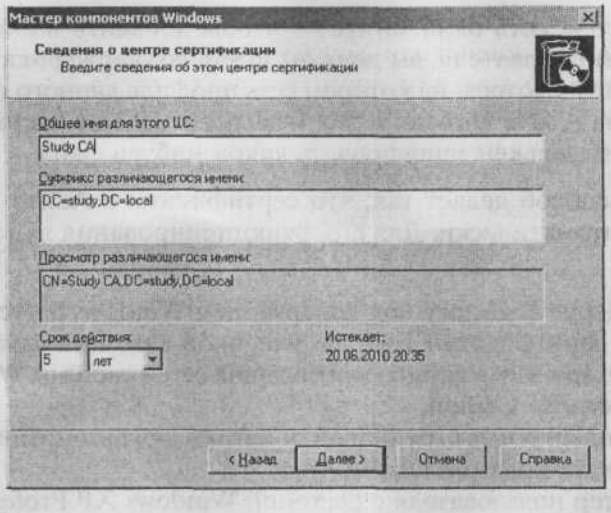


Рис. 22.3. *Задание основных параметров сертификационной службы*

Открытие доступа к зашифрованному файлу

Открытие доступа к зашифрованному файлу производится следующим образом:

1. Зарегистрируйтесь на PC001 как пользователь `efsuser`.
2. Откройте свойства зашифрованного файла. Затем на вкладке **Общие** нажмите кнопку **Дополнительно** и в диалоговом окне **Дополнительные атрибуты** около атрибутов шифрования нажмите кнопку **Подробно.** Откроется диалоговое окно **Подробности шифрования.** В части **Пользователи, которым разрешен доступ к этому файлу** обычно указан только пользователь, который зашифровал файл. Только он может добавить следующего пользователя.
3. Нажмите кнопку **Добавить.** В диалоговом окне **Выбрать пользователя** нажмите **Найти пользователя** и наберите в поле поиска `ITManager1`. Щелкните на **Проверить имена,** чтобы начать поиск пользователя `ITManager1`.
4. Выделите сертификат пользователя `ITManager1` и нажмите **OK**. Сертификат будет внесен в список, и пользователь `ITManager1` получит доступ к файлу.

Если вы будете пользоваться возможностью предоставления доступа по сети к зашифрованным файлам на практике, помните, что каждый пользователь, у которого есть доступ к зашифрованному файлу, может удалить вас из списка пользователей, имеющих доступ к этому файлу.

У этого способа есть один минус — чтобы добавить в список доступа следующего пользователя, вы должны иметь его сертификат. Его можно получить из компьютера, на котором есть профиль данного пользователя, или из домена Active Directory. Но чтобы сертификат открылся, пользователь сначала должен зашифровать какой-нибудь файл.

Следующий способ делает так, что сертификаты в Active Directory сохраняются автоматически. Для его функционирования вам понадобится следующее:

- Домен Active Directory под управлением Windows Server 2003.
- Шаблон сертификата EFS с разрешенной автоматической записью.
- Сертификационная служба для больших сетей системы Windows Server 2003 Enterprise Edition.
- Настроенный объект групповой политики для автоматической записи сертификата пользователями.
- Компьютер пользователя с системой Windows XP Professional.

Хотя мы и предполагаем, что у нас версия операционной системы Windows Server 2003 Standard Edition, все же давайте рассмотрим, хотя бы теоретически, действия для автоматического размещения сертификатов в Active Directory.

Действия будут следующие:

- Установка сертификационной службы большой сети — это мы уже проделали выше.
- Настройка сертификационной службы — состоит из создания и настройки шаблона сертификата.
- Настройка объекта групповой политики для автоматической записи сертификата.

Настройка сертификационной службы

Установленная нами сертификационная система способна создать любой сертификат для любого члена домена — не только пользователя, но и, например, компьютера или службы. Ее возможности очень обширны, но мы будем их использовать в достаточно малой степени. Сертификационную службу настроим таким образом, что она будет создавать сертификаты только для системы EFS и делать это автоматически.

Настройка шаблона сертификата:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Откройте пустую консоль MMC и добавьте оснастку **Шаблоны сертификатов.**
3. Раскройте контейнер **Шаблоны сертификатов** и в правом окне консоли убедитесь, что у шаблона **Базовое шифрование EFS** в столбце

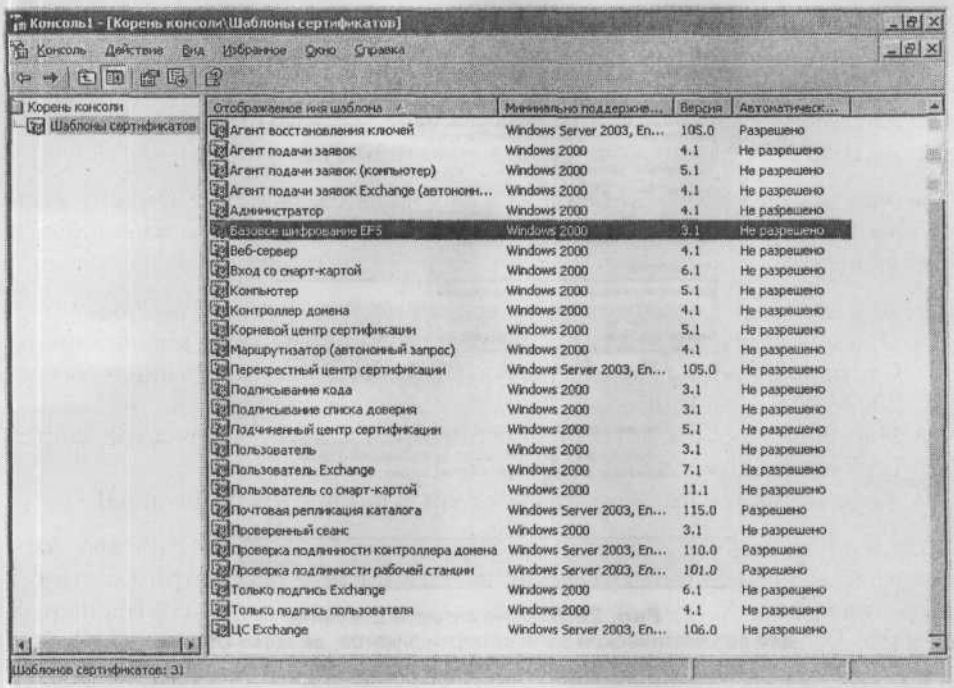


Рис. 22.4. *Шаблоны сертификатов*

Автоматическая подача заявок (Autoenrollment) стоит значение **Не разрешено (Not Allowed).** Это нам, конечно, не подходит, поэтому создадим собственный шаблон, в котором будет разрешена автоматическая запись.

4. Щелкните правой кнопкой мыши по шаблону **Базовое шифрование EFS** и из контекстного меню выберите команду **Скопировать шаблон.** Откроется диалоговое окно **Свойства нового шаблона.**
5. На вкладке **Общие** введите в поле **Отображаемое имя шаблона** строку «Автоматическая запись сертификатов для EFS», а в поле **Имя шаблона** — «AutoEnrollBasicEFS». Все остальное оставьте без изменений.
6. На вкладках **Обработка запроса** и **Имя субъекта** ознакомьтесь со значениями по умолчанию, оставив их без изменений. Перейдите на вкладку **Безопасность.**
7. Для автоматической записи сертификатов необходимы разрешения «Чтение» (Read), «Заявка» (Enroll) и «Автоматическая подача заявок» (Autoenroll). Разрешение читать пользователи домена получают благодаря членству в группе «Authenticated Users», остальные разрешения — через группу «Domain Users».

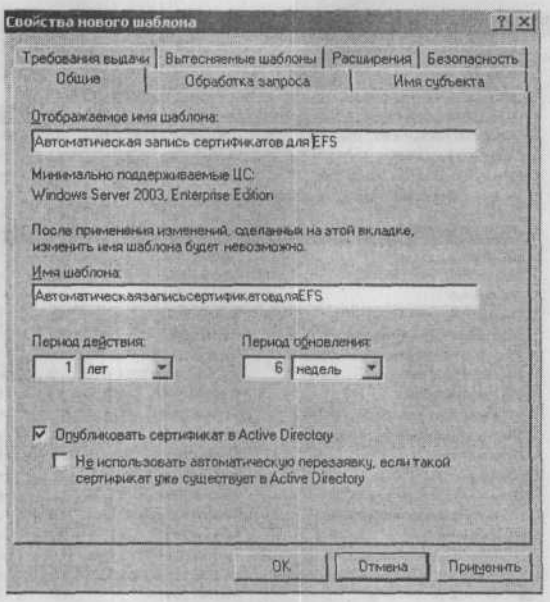


Рис. 22.5. *Окно свойств шаблона для автоматической записи сертификатов, вкладка Общие*

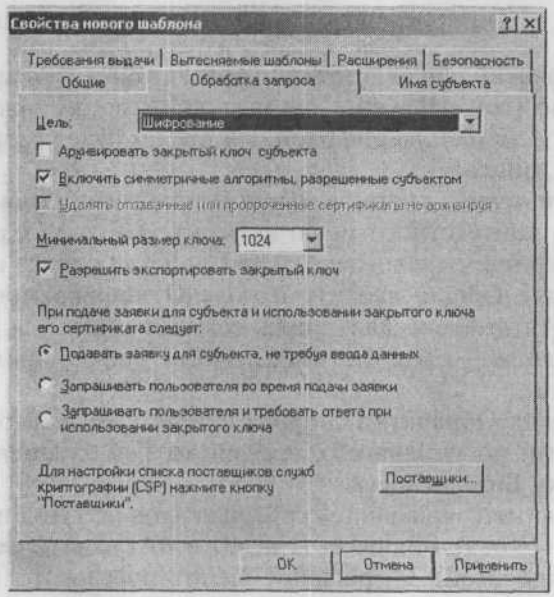


Рис. 22.6. *Окно свойств шаблона для автоматической записи сертификатов, вкладка Обработка запроса*

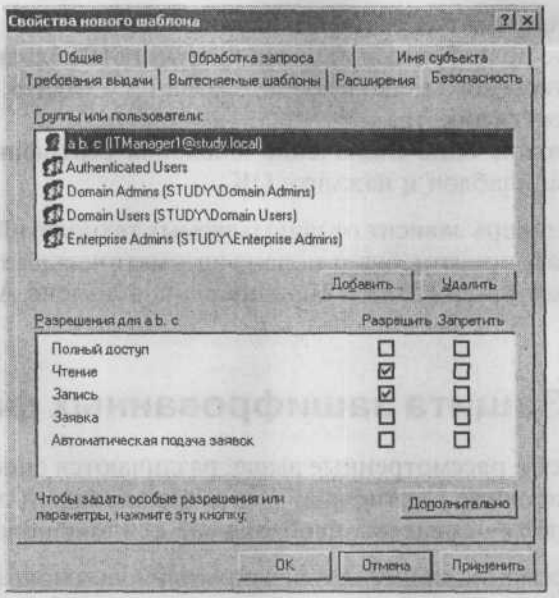


Рис. 22.7. *Окно свойств шаблона для автоматической записи сертификатов, вкладка Безопасность*

Настройка групповой политики

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль **Active Directory — пользователи и компьютеры.**
2. На уровне домена создайте новый объект групповой политики с именем «Автоматическая запись сертификатов EFS».
3. В новом объекте раскройте ветвь **Конфигурация пользователя\Конфигурация Windows\Параметры безопасности\Политики открытого ключа.**
4. Щелкните по политике **Параметры автоматической подачи заявок** и в диалоговом окне **Параметры** установите флажки **Подавать заявки на сертификаты автоматически, Обновлять сертификаты с истекшим сроком действия...** и **Обновлять сертификаты на основе шаблонов сертификатов**.
5. Закройте все диалоговые окна.

Теперь необходимо добавить этот шаблон к шаблонам центра сертификации. Это можно сделать только с помощью утилиты **Сертификационный центр**, из сертификационной службы системы Windows Server 2003, Enterprise Edition. Следующее действие в нашей учебной сети осуществить нельзя:

1. Зарегистрируйтесь на компьютере с системой Windows Server 2003, Enterprise Edition как администратор.

2. Запустите утилиту **Сертификационный центр**.
3. Щелкните правой кнопкой мыши по пункту **Шаблоны сертификатов** и из контекстного меню выберите команду **Создать → Выдаваемый шаблон сертификата**.
4. В диалоговом окне **Включение шаблонов сертификатов** выберите созданный шаблон и нажмите **OK**.

Все остальное теперь зависит от используемых технологий. В ходе применения групповых политик будет подана автоматическая заявка на сертификат, она будет утверждена и опубликована в домене Active Directory.

22.4. Защита зашифрованных файлов

Три возможности, рассмотренные выше, различаются способом создания и записи сертификата. Сертификат — это подписанный открытый ключ, а открытый ключ — средство, необходимое для шифрования файла.

Если для шифрования применяется открытый ключ пользователя, то для последующего дешифрования (которое невидимым образом протекает на заднем плане при любых манипуляциях с файлом) применяется закрытый ключ пользователя.

Где хранится закрытый ключ пользователя? Это вопрос, который требует понимания процессов шифрования и дешифрования. Закрытый ключ пользователя является неотъемлемой частью его профиля.

Это означает следующее:

- Если пользователь лишится профиля, то он потеряет также свой закрытый ключ.
- Для пользователя с локальным профилем на каждом компьютере, где он шифрует данные, создается отдельный закрытый ключ.
- Если пользователь копирует зашифрованный файл на другой компьютер с файловой системой NTFS, в компьютере назначения будет создан его профиль с закрытым ключом.

Давайте посмотрим, какие последствия на практике может иметь потеря закрытого ключа. Прежде чем удалить закрытый ключ, архивируем его:

1. Зарегистрируйтесь на компьютере PC001 как пользователь `efsuser`.
2. Откройте пустую консоль MMC и добавьте в нее оснастку **Сертификаты** для своей учетной записи.
3. Раскройте ветвь **Сертификаты — текущий пользователь\Личные\ Сертификаты**. В правом подокне консоли щелкните правой кнопкой мыши по сертификату `efsuser`, у которого в столбце **Кем выдан** стоит также значение `efsuser`, и из контекстного меню выберите

команду **Все задачи → Экспорт**. Запустится Мастер экспорта сертификатов. Нажмите **Далее**.

4. В диалоговом окне **Экспортирование закрытого ключа** поставьте флажок в поле **Да, экспортировать закрытый ключ** и нажмите **Далее**. Переключатель **Экспортирование закрытого ключа** становится активным только в случае, если вы являетесь собственником закрытого ключа. В противном случае он будет серого цвета.
5. В диалоговом окне **Формат экспортируемого файла** оставьте предложенные значения и нажмите **Далее**.
6. В диалоговом окне **Пароль** введите и подтвердите пароль для защиты закрытого ключа и продолжайте нажатием **Далее**.
7. В диалоговом окне **Имя файла экспорта** укажите путь к папке, где вы хотите сохранить свой закрытый ключ (например, `C:\efsuser\key`). Нажмите **Далее**.
8. В диалоговом окне **Завершение мастера экспорта сертификатов** просмотрите указанную информацию и нажмите **Готово**. Отобразится сообщение об успешном завершении экспорта.

Нужно отметить, что теперь экспортированный закрытый ключ находится в таком месте, до которого злоумышленнику добраться значительно проще, чем до профиля пользователя. Реальный ключ следует тут же записать на компакт-диск, спрятать диск в сейф и удалить файл с компьютера.

Теперь попробуем получить доступ к зашифрованному файлу:

1. Если вы зарегистрированы на компьютере PC001 как пользователь `efsuser`, убедитесь, что у вас нет проблем с открытием зашифрованного файла.
2. Перерегистрируйтесь на компьютере PC001 как администратор.
3. Правой кнопкой мыши щелкните по значку **Мой компьютер** и откройте его свойства. Затем на вкладке **Дополнительно** в секции **Профили пользователей** нажмите кнопку **Параметры**.
4. В диалоговом окне **Профили пользователей** выберите профиль пользователя `STUDY\efsuser` и нажмите кнопку **Удалить**. Подтвердите удаление нажатием кнопки **Да**.
5. Снова перерегистрируйтесь как пользователь `efsuser`. Регистрация займет некоторое время, так как создается новый профиль пользователя.
6. Попробуйте открыть собственный зашифрованный файл в папке `C:\efsuser`. Естественно, у вас это не получится и появится сообщение об ошибке «Отказано в доступе».

Это доказательство того, что:

- Для расшифровки файла вам нужен ваш закрытый ключ.
- Закрытый ключ является частью профиля пользователя.

Какие же есть возможности доступа к зашифрованному файлу? Если закрытый ключ пользователя `efsuser` хранится где-то в сейфе, то достаточно будет импортировать его обратно в профиль. Если же закрытый ключ пропал совсем, то восстановить доступ будет значительно труднее: придется воспользоваться так называемым Агентом восстановления ключей.

22.5. Восстановление доступа к зашифрованному файлу

1. Зарегистрируйтесь на компьютере PC001 как пользователь `efsuser`.
2. Запустите консоль MMC и добавьте к ней оснастку **Сертификаты.**
3. Раскройте ветвь **Сертификаты — текущий пользователь\Личные.** Убедитесь, что здесь нет ни одного сертификата (так как профиль `efsuser` создан только что).
4. В правом окне консоли щелкните правой кнопкой мыши и из контекстного меню выберите команду **Все задачи → Импорт.** Запустится Мастер импорта сертификатов. Нажмите **Далее.**
5. В диалоговом окне **Импортируемый файл** нажмите кнопку **Обзор** и найдите файл `KEY.PFX` (это ключ, экспортированный в предыдущем параграфе). Нажмите **Далее.**
6. В диалоговом окне **Пароль** введите пароль, который вы использовали при экспорте ключа и отметьте **Пометить этот ключ как экспортируемый...,** нажмите **Далее.**
7. В диалоговом окне **Хранилище сертификатов** оставьте предложенные значения и нажмите **Далее.**
8. В диалоговом окне **Завершение мастера импорта сертификатов** нажмите **Готово.** Отобразится сообщение об успешном выполнении импорта.
9. В окне консоли теперь вы снова увидите собственный сертификат для шифрования.
10. Попробуйте открыть зашифрованный файл. Теперь это вам удастся.

Мы видим, что получить доступ к зашифрованным файлам несложно. Чтобы не столкнуться с проблемами доступа к зашифрованным файлам, достаточно заранее экспортировать свой закрытый ключ.

Проблема в том, что спасение своих файлов требует от пользователей некоторой квалификации, на которую вы, как администратор, рассчитывать не можете. Вам придется самому экспортировать закрытые ключи пользователей при помощи Агента восстановления.

22.6. Структура зашифрованного файла

Для правильного понимания принципа действий необходимо знать, что происходит «внутри» при шифровании и расшифровывании файла:

1. Пользователь (например, `efsuser`) отдает команду зашифровать файл.
2. Система Windows XP Professional генерирует случайный ключ (FEK, File Encryption Key), которым зашифрует содержимое файла.
3. Система берет открытый ключ пользователя, шифрует им ключ FEK и результат сохраняет в поле расшифровки данных (DDF, Data Decryption Field).
4. Далее система берет общий ключ Агента восстановления данных, шифрует им ключ FEK и результат сохраняет в поле восстановления данных (DRF, Data Recovery Field).
5. Эти действия повторяются для всех Агентов восстановления данных.
6. Система закрывает файл и сохраняет его на диске.

Возможно, вас удивила информация о том, что при помощи открытого ключа шифруется ключ FEK вместо содержимого файла. Это логично, так как в противном случае к файлу не смог бы получить доступ никто, кроме пользователя, который его зашифровал. Все бы работало, но только до потери закрытого ключа пользователя.

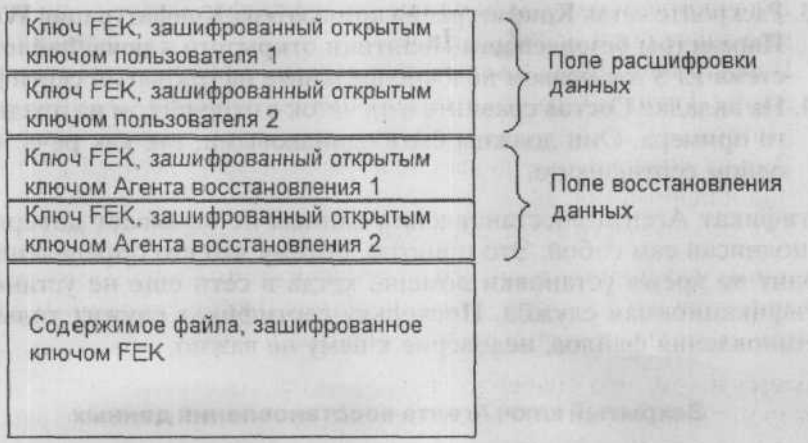


Рис. 22.8. *Структура зашифрованного файла*

Если пользователю нужно открыть файл, он использует закрытый ключ, расшифрует с его помощью ключ FEK, которым затем расшифрует файл.

22.7. Агент восстановления данных

Агент восстановления данных в исходной установке один на весь домен.

1. Зарегистрируйтесь на PC001 как пользователь `efsuser`.
2. Откройте свойства зашифрованного файла, нажмите кнопку **Дополнительно** и в диалоговом окне **Дополнительные атрибуты** нажмите **Подробно.** Отобразится сообщение о том, какие ключи являются частью поля расшифровывания данных (верхняя часть) и поля восстановления данных (нижняя часть).
3. В нижней части диалогового окна приведен сертификат Агента восстановления данных. Запомните его так называемый отпечаток.

Агент восстановления данных автоматически пропишется в каждый зашифрованный файл, как этого требует объект групповой политики по умолчанию.

Поиск Агента восстановления

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль **Active Directory — пользователи и компьютеры.**
2. Откройте объект групповой политики по имени «Default Domain Policy».
3. Раскройте ветвь **Конфигурация компьютера\Конфигурация Windows\ Параметры безопасности\Политики открытого ключа\Файловая система EFS** и в правом подокне щелкните на открытый сертификат.
4. На вкладке **Состав** сравните отпечаток с отпечатком из предыдущего примера. Они должны быть одинаковыми, так как речь идет об одном сертификате.

Сертификат Агента восстановления данных не вызывает доверия, так как подписан сам собой. Это понятно, потому что его определение происходит во время установки домена, когда в сети еще не установлена сертификационная служба. Поскольку сертификат служит только для восстановления файлов, недоверие к нему не важно.

Закрытый ключ Агента восстановления данных

Агент восстановления данных является последним средством, к которому пользователи могут в случае необходимости обратиться. Чтобы было возможно расшифровать файл пользователя, необходим закрытый ключ.

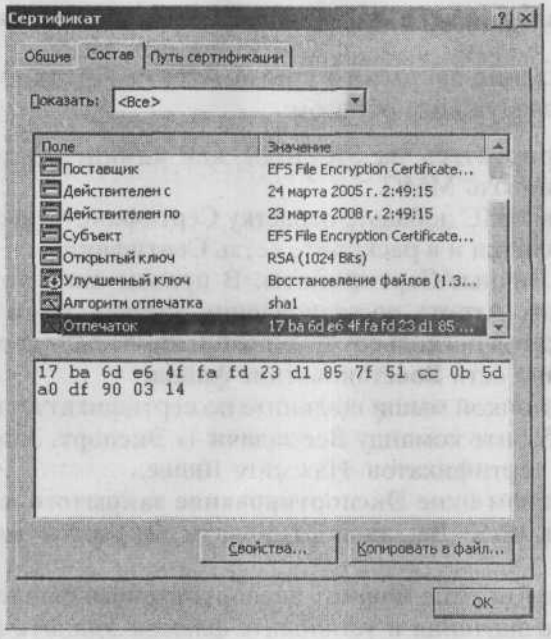


Рис. 22.9. *Сертификат Агента восстановления данных и его отпечаток*

Поэтому очень важно как можно раньше провести экспорт закрытого ключа, так как в противном случае Агент восстановления данных может быть похоронным агентом.

Закрытый ключ Агента восстановления данных хранится в профиле администратора на первом из установленных контроллеров домена, и больше нигде. Чтобы обезопасить этот ключ от несанкционированного доступа, настоятельно рекомендуется экспортировать его на съемный носитель и стереть из компьютера.

Экспорт ключа — это понятно. Зачем, однако, удалять ключ из компьютера? Для этого есть две причины.

Первая причина — это обеспечение конфиденциальности данных пользователей. Если оставить ключ Агента восстановления данных на компьютере, его может найти любой администратор домена и просмотреть с его помощью любой зашифрованный файл в домене.

Другой причиной является безопасность самого ключа. Если ключ хранится только в сейфе, злоумышленнику будет труднее до него добраться.

Экспорт и удаление закрытого ключа Агента восстановления данных

Экспорт и удаление закрытого ключа Агента восстановления данных производится следующим образом:

1. Зарегистрируйтесь на SRVR001 как администратор и запустите пустую консоль MMC.
2. В консоль MMC добавьте оснастку **Сертификаты** своей собственной учетной записи и в раскройте ветвь **Сертификаты — текущий пользователь\Личные\Сертификаты.** В правом окне консоли появится сертификат Агента восстановления данных. Если в правом окне сертификатов несколько, будем работать с тем, у которого в столбце **Назначения** есть **Восстановление файла.**
3. Правой кнопкой мыши щелкните по сертификату и из контекстного меню выберите команду **Все задачи → Экспорт.** Запустится Мастер экспорта сертификатов. Нажмите **Далее.**
4. В диалоговом окне **Экспортирование закрытого ключа** поставьте флажок в поле **Да, экспортировать закрытый ключ** и нажмите **Далее**.
5. В диалоговом окне **Формат экспортируемого файла** оставьте предложенные значения и установите флажок **Удалить закрытый ключ после успешного экспорта.** Продолжайте нажатием **Далее.**
6. В диалоговом окне **Пароль** введите и подтвердите пароль. Затем щелкните на **Далее.**
9. В диалоговом окне **Имя файла экспорта** укажите путь к папке, где вы хотите сохранить свой закрытый ключ (например, `C:\RA`), и имя файла (например, `RA.PFX`). Затем нажмите **Далее.**

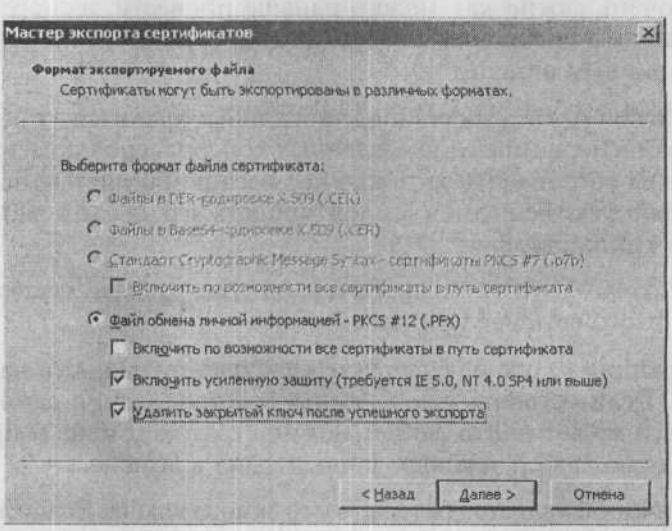


Рис. 22.10. *Диалоговое окно Формат экспортируемого файла*

7. В диалоговом окне **Завершение мастера экспорта сертификатов** просмотрите указанную информацию и нажмите **Готово.** Отобразится сообщение об успешном завершении экспорта.
8. Файл `RA.PFX` скопируйте на дискету (а еще лучше — на компакт-диск) и удалите из компьютера (в том числе и из **Корзины**). Диск и листок с паролем, защищающим закрытый ключ, положите в конверт, запечатайте и спрячьте в сейф.

Порядок восстановления зашифрованных данных

Если пользователь лишится закрытого ключа и таким образом потеряет доступ к зашифрованному файлу, он попросит вас о помощи. В таком случае действуйте следующим образом:

1. Достаньте из сейфа закрытый ключ Агента восстановления данных и запишитесь в журнале безопасности.
2. На компьютере пользователя зарегистрируйтесь как администратор.
3. Запустите консоль MMC и добавьте в нее оснастку **Сертификаты** своей учетной записи. В сертификат импортируйте закрытый ключ Агента восстановления данных.
4. Теперь перейдите к свойствам зашифрованного файла и снимите атрибут шифровки.
5. При помощи консоли сертификата проведите экспортирование закрытого ключа и последующее удаление из компьютера.
6. Диск с закрытым ключом Агента верните в сейф и сообщите пользователю о перешифровке файла.

22.8. Итоги

Операционные системы Microsoft безопасны, даже в исходной конфигурации. При переходе от системы Windows 2000 к Windows Server 2003 произошли большие изменения, и безопасность новой системы намного выше.

Сразу после инсталляции домена необходимо провести некоторые действия, связанные с системой шифровки файлов EFS. Имеется в виду прописка Агента восстановления данных, экспорт и последующее удаление из системы закрытых ключей.

Если пользователи работают в Windows XP Professional и хотят делить доступ к зашифрованным файлам, нужно установить в сети сертификационную службу Windows Server 2003 Enterprise Edition, которая будет автоматически создавать нужные сертификаты.

Также хорошо запретить шифрование там, где это не нужно. Это общие папки и документы, к которым должно иметь доступ несколько пользо-

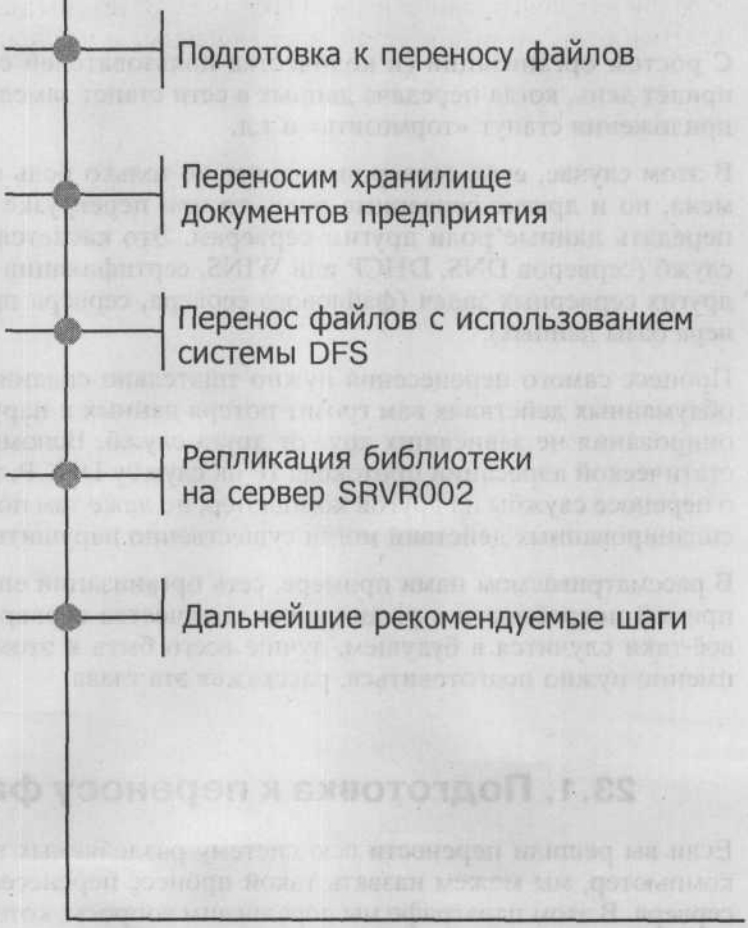
вателей. Если необходимо запретить шифрование только на одном компьютере, можно это сделать при помощи объекта групповой политики.

Обычно в системе EFS нужно думать о том, что речь идет об очень сильном механизме безопасности данных. Точно так же, как файлы можно просто и быстро зашифровать, их можно быстро потерять. Об этом помните всегда и защищайте свои ключи.

Состояние сети

Самым заметным изменением в сети стала установка сертификационной службы, которая используется для выдачи сертификатов и генерирования ключей для шифрования и дешифрования. Затем мы экспортировали закрытый ключ Агента восстановления данных и удалили его из домена.

Глава 23 Когда одного сервера недостаточно



С ростом организации (и количества пользователей сети) неизбежно придёт день, когда передача данных в сети станет замедленной, сетевые приложения станут «тормозить» и т.д.

В этом случае, если сервер выполняет не только роль контроллера домена, но и другие серверные роли, то при перегрузке домена следует передать данные роли другим серверам. Это касается как системных служб (серверов DNS, DHCP или WINS, сертификации и других), так и других серверных задач (файлового сервера, сервера приложений, сервера базы данных).

Процесс самого перенесения нужно тщательно спланировать. При необдуманных действиях вам грозит потеря данных и нарушение функционирования не зависящих друг от друга служб. Вспомните переход со статической адресации протокола IP на службу DHCP: там не шло речи о переносе службы на другой компьютер, но даже там последствия плохо спланированных действий могли существенно нарушить работу сети.

В рассматриваемом нами примере, сеть организации ещё не созрела до прямой потребности в расширении количества серверов. Но если это всё-таки случится в будущем, лучше всего быть к этому *готовым*. Как именно нужно подготовиться, расскажет эта глава.

23.1. Подготовка к переносу файлов

Если вы решили перенести всю систему разделяемых папок на другой компьютер, мы можем назвать такой процесс перенесением файлового сервера. В этом параграфе мы перечислим вопросы, которые нужно продумать заранее.

23.1.1. Производительность компьютера

Самой распространённой причиной перенесения любой функции с одного компьютера на другой является низкий уровень производительности исходного компьютера. При оценке производительности компьютера обычно принимают во внимание следующие компоненты оборудования:

- Процессор
- Память
- Дисковая подсистема
- Сетевой интерфейс.

В большинстве случаев администраторы забывают о быстродействии дисковой подсистемы. При покупке нового оборудования их интересует объём и количество дисков. Этого недостаточно, поскольку важную роль играет также способ организации дисков в массив RAID, размер дискового кэша и многое другое.

Указанные составляющие существенны для всех компьютеров. На серверах, однако, в зависимости от выполняемой сервером роли на одни характеристики следует обратить особое внимание, а другими можно пренебречь. Например, в то время как для файлового сервера будет важен размер памяти и производительность дисковой подсистемы, для сервера DNS или DHCP будет гораздо важнее скорость процессора и сетевого интерфейса.

Гораздо хуже обстоит дело в случае, когда один сервер совмещает несколько ролей. Что выгоднее для повышения производительности — купить более быстрый процессор или добавить памяти? Добавить еще один сетевой адаптер или ещё один диск? Однозначного ответа на эти вопросы не существует.

У файлового сервера необходимо обращать особое внимание на *достаточный размер оперативной памяти* и на *объем и быстродействие жёстких дисков*. Здесь не играет особой роли скорость процессора, и, если файлы не требуют высокой скорости передачи по сети, то и сетевой интерфейс. Какой размер оперативной памяти считать достаточным, сказать заранее невозможно: минимальный размер определяется системными требованиями, максимальный — чаще всего техническими или финансовыми возможностями предприятия.

Под быстродействием жёстких дисков подразумевается не только время доступа, но также и способ организации дискового массива. Дополнительная информация о возможностях организации дисков приведена в главе 24.

23.1.2. Перенос файлов и разрешения NTFS

Разрешения NTFS определяют, кто и как может работать с данным объектом. Это свойства конкретного объекта (файла, папки, принтера...), и важно, чтобы при переносе объекта его разрешения не изменились. Поэтому администратор обязан твердо знать, что происходит с разрешениями при манипуляциях с файлами.

Разрешения NTFS и копирование

Копия объекта не сохраняет разрешений оригинала, а наследует их от той папки, в которую скопирован объект. То есть, если вы скопировали файл, к которому некоторый пользователь имел доступ только на чтение, в папку, к которой у него есть полный доступ, то он получит полный доступ к копии файла.

Разрешения NTFS и перемещение

Если объект перемещен с одного раздела NTFS на другой, то с его разрешениями происходит то же, что при копировании: они наследуются от родительской папки.

Если объект перемещен в пределах раздела, то он сохраняет разрешения вне зависимости от разрешений родительской папки назначения.

Из сказанного выходит, что и копирование, и перемещение объектов между компьютерами приведут к одному и тому же — файлы лишатся изначальных прав доступа и унаследуют полномочия родительской папки.

23.1.3. Перемещение зашифрованных файлов

С зашифрованными файлами может манипулировать только тот, кто их зашифровал. Остальные пользователи, какие бы полномочия они ни имели, перемещать этот файл не могут. Исключением может служить разве что Агент восстановления, но в хорошо защищенной сети его закрытый ключ удалён из домена, и он тоже не сможет ничего сделать.

При копировании на другой компьютер зашифрованный файл сначала дешифруется, потом передается по сети и в компьютере назначения снова зашифровывается. Там создается профиль пользователя, которому принадлежит зашифрованный файл, поскольку закрытый ключ является его частью. Чтобы разрешить шифровать файлы на удалённом компьютере, в свойствах исходного компьютера должен быть установлен флажок **Доверять компьютеру делегирование** (рис. 23.1). Обычно этот флажок установлен только у контроллера домена.

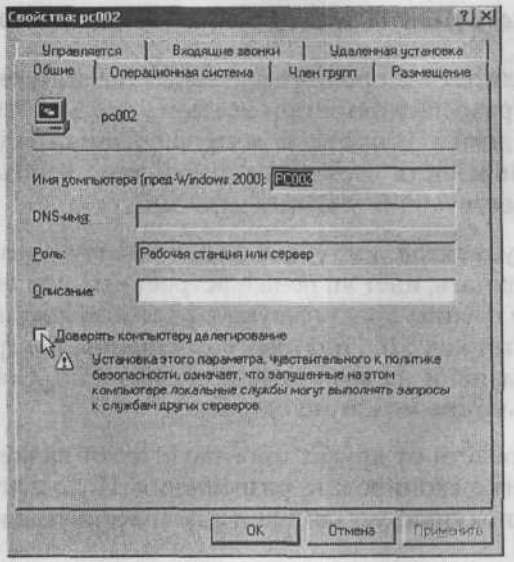


Рис. 23.1. *Вкладка Общие в окне свойств учётной записи компьютера*

23.1.4. Копирование и перемещение сжатых файлов

Сжатие является ещё одной особенностью системы NTFS. Атрибут сжатия файла при копировании и перемещении ведет себя так же, как разрешения NTFS. Если папка назначения сжата, файл при копировании тоже будет сжат. Если папка назначения не сжата, файл при копировании декомпрессируется.

При перемещении между разделами атрибут сжатия ведет себя так же, как при копировании, перемещение в пределах раздела сохраняет атрибут сжатия файлов.

23.1.5. Варианты перемещения

Вышеизложенная информация является основной частью для успешного планирования перемещения общих папок и файлов. Одна из самых распространенных ошибок администраторов — забывать о том, что при перемещении файлов теряются их разрешения и некоторые атрибуты, а также о том, что чужие зашифрованные файлы перемещать нельзя.

Возможно ли сохранить атрибуты перемещаемых файлов?

Инструменты от сторонних производителей

Существуют утилиты от сторонних производителей, умеющие копировать файлы вместе с разрешениями при условии, что компьютер назначения входит в тот же домен. В противном случае в списке субъектов доступа на вкладке **Безопасность** свойств скопированного объекта будут лишь коды SID несуществующих учётных записей.

Если в списке субъектов доступа к файлу числятся локальные группы, необходимо различать, идёт ли речь о встроенных или собственных группах. Встроенные группы присутствуют на каждом компьютере, и все они имеют одинаковый код SID, поэтому разрешения, настроенные для них, будут действительны и на компьютере назначения. Собственных групп на другом компьютере может не оказаться.

Достоинством средств от других производителей является возможность сравнительно легко скопировать разрешения. Недостатком является необходимость их покупки, установки и администрирования.

Системные средства

В главе 16 вы познакомились с утилитой архивации (**NTBackup.exe**). Многие администраторы недооценивают ее возможности и используют ее только для резервного копирования системы, а ведь она позволяет убить всех зайцев, о которых говорится в этом параграфе. Если можно архивировать и восстанавливать файлы вместе с их разрешениями и другими атрибутами, а также зашифрованные файлы, то что мешает восстановить их на диск другого компьютера?

Напомним, что для архивирования системы необходимы полномочия члена группы администраторов домена или операторов архива (Backup Operators).

23.1.6. Общие папки

Если вам нужно переместить разделяемые папки на другой сервер, вы наверняка не захотите лишиться настроенных прав сетевого доступа. Эти права являются свойством не папки, а компьютера, который открыл ее для доступа по сети. Вы найдёте их в ветви реестра HKEY_LOCAL_MACHINE (рис. 23.2).

В ключе `Shares` хранится информация о свойствах объекта, разрешенного для доступа через сеть, т.е. о его названии, максимальном количестве подключаемых одновременно пользователей и т.п. В подключе `Security` хранится информация о правах доступа.

Как всю эту информацию перенести на другой компьютер? Однозначно, не с помощью архивации состояния системы (System State). Ее можно восстановить только как единое целое, так что новый компьютер у нас бы был всего лишь копией старого (включая то же название, те же коды SID и тому подобное). Это нам, конечно, не годится, так что будем искать иной способ. Например, можно записать данные из ключа Shares, а на компьютере назначения ввести их, вручную редактируя реестр. Если у вас одна-две разделяемые папки, то это достаточно быстрая процедура.

Если же у вас их десятки, то проще будет на исходном компьютере экспортировать ключ Shares в файл REG, при необходимости отредактировать этот текстовый файл и импортировать его в реестр на компьютере назначения.

Следует спланировать время перемещения общих папок с учетом того, что на это время они окажутся недоступны для пользователей.

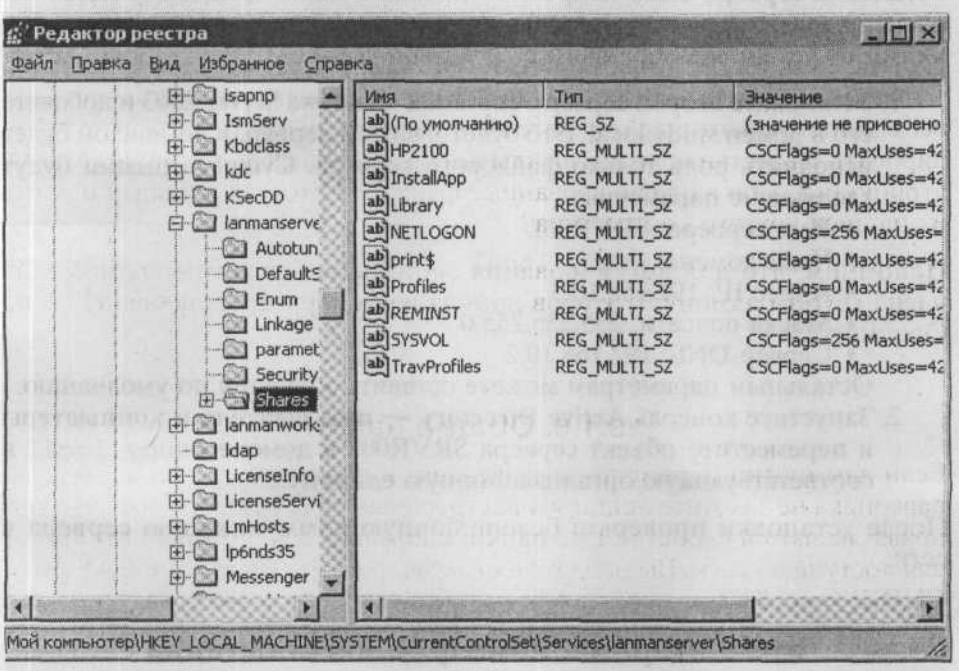


Рис. 23.2. *Свойства разделяемой папки в системном реестре*

23.2. Переносим хранилище документов предприятия

Процесс перенесения хранилища будет состоять их следующих шагов:

- Установка и настройка второго сервера (SRVR002).
- Архивация структуры папок и важных ключей реестра.
- Запрещение доступа к файлам на прежнем месте.
- Восстановление структуры на новом сервере.
- Разрешение доступа к структуре на новом сервере.

Альтернативный подход:

- Установка и настройка второго сервера.
- Использование системы DFS (Distributing File System) для перенесения содержимого общих папок.

23.2.1. Установка и настройка второго сервера

Установка сервера была подробно описана в главе 1, поэтому здесь мы очертим необходимые шаги только пунктирно. За недостающими сведениями об установке обращайтесь к первой главе.

1. Установите второй сервер с системой Windows Server 2003 и добавьте его в домен study.local. Это будет рядовой сервер, в домене он будет исполнять роль только файлового сервера. Существенными будут следующие параметры:
   - Имя сервера: SRVR002
   - Член домена: `study.local`
   - Адрес IP: 192.168.10.3
   - Маска подсети: 255.255.255.0
   - Сервер DNS: 192.168.10.2

   Остальным параметрам можете оставить значения по умолчанию.
2. Запустите консоль **Active Directory — пользователи и компьютеры** и переместите объект сервера SRVR002 в домене `study.local` в соответствующую организационную единицу.

После установки проверьте безошибочную коммуникацию сервера в сети.

23.2.2. Перенесение файлов способом архивации и восстановления

Этот метод планируйте на то время, когда пользователи не будут работать с файлами. Весь процесс будет состоять из нескольких отдельных шагов,

оптимизированных таким образом, чтобы он был как можно более простым и как можно меньше ограничивал пользователей.

Архивация ключей реестра

Архивация ключей реестра производится следующим образом:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Запустите редактор реестра **REGEDIT.EXE** и перейдите в ветвь **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares**.
3. Выполните команду **Файл → Экспорт** и в диалоговом окне **Экспорт файла реестра** задайте название файла `LIB.REG` и сохраните его временно на диске C:.

Редактирование ключей реестра

Поскольку из всех разделяемых папок нас будет интересовать только папка `Library` (известная в сети как «Библиотека»), необходимо отредактировать экспортируемый файл так, чтобы в компьютере назначения лишний раз не появлялись сообщения о недостающих общих папках.

1. Откройте файл `LIB.REG` в Блокноте. Это обычный текстовый файл, фрагмент которого приведен ниже.
2. Удалите из файла `LIB.REG` все записи, кроме относящихся к папке `Library`, и сохраните файл под тем же именем.

```
«SYSVOL»=hex:01,00,04,80,5c,00,00,00,6c,00,00,00,00,00,00,00,14,00,00,00,02,00,\
48,00,03,00,00,00,00,00,14,00,a9,00,12,00,01,01,00,00,00,00,00,01,00,00,00,\
00,00,00,18,00,ff,01,1f,00,01,02,00,00,00,00,00,05,20,00,00,00,20,02,00,00,\
00,00,14,00,ff,01,1f,00,01,01,00,00,00,00,00,05,0b,00,00,00,01,02,00,00,00,\
00,00,05,20,00,00,00,20,02,00,00,01,01,00,00,00,00,00,05,12,00,00,00
«NETLOGON»=hex:01,00,04,80,48,00,00,00,58,00,00,00,00,00,00,00,14,00,00,00,02,\
00,34,00,02,00,00,00,00,00,14,00,a9,00,12,00,01,01,00,00,00,00,00,01,00,00,\
00,00,00,00,18,00,ff,01,1f,00,01,02,00,00,00,00,00,05,20,00,00,00,20,02,00,\
00,01,02,00,00,00,00,00,05,20,00,00,00,20,02,00,00,01,01,00,00,00,00,00,05,\
12,00,00,00
«Library»=hex:01,00,04,80,30,00,00,00,40,00,00,00,00,00,00,00,14,00,00,00,02,\
00,1c,00,01,00,00,00,00,00,14,00,ff,01,1f,00,01,01,00,00,00,00,00,05,0b,00,\
00,00,01,02,00,00,00,00,00,05,20,00,00,00,20,02,00,00,01,05,00,00,00,00,00,\
05,15,00,00,00,0d,a5,06,54,aa,36,59,b7,7d,2a,e2,fe,01,02,00,00
```

Запрещение доступа к папке и архивация ее содержимого

Даже если вы предупредили пользователей о своих действиях и объяснили им, как себя вести, вполне возможно, что некоторые пользователи вас не послушаются и продолжат работу с сетевыми файлами.

Чтобы предупредить их еще раз о своей работе с этими файлами, можете поступить следующим образом:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Щелкните правой кнопкой мыши по значку **Мой компьютер** и запустите консоль **Управление компьютером**. Правой кнопкой мыши щелкните по контейнеру **Общие папки** и из контекстного меню выберите команду **Все задачи → Отправка сообщения консоли**. Отобразится диалоговое окно, в котором вы введете текст сообщения о том, что начинаете работать с файлами и не отвечаете за возможную потерю данных. Разошлите это сообщение нажатием кнопки **Отправить**.

Примечание.

Успешная отсылка и доставка сообщения компьютерам требует функционирующей службы **Messenger**. Поскольку эта служба в исходном состоянии в системах Windows Server 2003 отключена, рассылка сообщений может стать невозможной.

3. Отобразите свойства папки `C:\Library` и снимите флажок **Открыть общий доступ к этой папке**.
4. Запустите утилиту **Архивация** (**NTBackup.exe**) и проведите полную архивацию папки «Library». Архив сохраните локально на компьютере в файле `LIBRARY.BKF`.

Восстановление содержимого и разрешение доступа к нему на новом месте

Восстанавливать архив папки `Library` мы будем на новый сервер. Потом мы проверим, сохранились ли разрешения NTFS, и, добавив данные в реестр, сделаем папку общей.

1. Зарегистрируйтесь на SRVR002 как администратор.
2. Запустите утилиту **Архивация**.
3. Восстановите файл `LIBRARY.BKF` с диска C: компьютера SRVR001 (путь к файлу `\\SRVR001\c$\LIBRARY.BKF`).
4. Щелкните правой кнопкой мыши по только что восстановленной папке `C:\Library`, выберите команду **Свойства** и перейдите на вкладку **Безопасность**. Поскольку восстановились также разрешения NTFS, список субъектов доступа и их прав должен совпадать с таким же списком на компьютере SRVR001.

Сетевые имена и права сетевого доступа для папки `Library` и ее подпапок скопируем путем экспорта соответствующего ключа реестра на компьютере SRVR001 и импорта его в реестр на компьютере SRVR002:

1. В компьютере SRVR002 откройте папку `\\SRVR001\c$`. Найдите файл `LIB.REG` и запустите его.
2. На вопрос, хотите ли вы импортировать информацию в реестр, ответьте нажатием кнопки **Да**. Нажатием **OK** закройте сообщение с информацией об успешной записи информации из файла `LIB.REG` в реестре.
3. Перезагрузите компьютер SRVR002. После перезагрузки папка `Library` получит те же права сетевого доступа, что на старом месте.

Примечание.

Перезагрузка после изменения реестра необходима только тогда, когда новые ключи и значения вы импортировали. Если вы вводили их вручную с помощью утилиты REGEDIT, изменения вступят в силу немедленно.

Что получилось? До сих пор хранилище документов предприятия было доступно по UNC-пути `\\SRVR001\Library`, теперь же мы задали для него путь `\\SRVR002\Library`. Осталось переучить пользователей «ходить другим путем».

Если пользователи подключают сетевой диск через сценарий регистрации, достаточно заменить путь в сценарии, и они даже не заметят перехода на новый файловый сервер.

23.3. Перенос файлов с использованием системы DFS

Настройка автоматической репликации между двумя общими папками

Файловая система DFS была впервые представлена в системах Windows 2000. В системе Windows Server 2003 она была расширена несколькими функциями, которые, однако, нам в дальнейшем не понадобятся. Ее можно считать своего рода «дорожной картой», упрощающей ориентацию и доступ пользователей к общим папкам, которые могут быть разбросаны по разным серверам в сети.

Файловая система DFS имеет всегда так называемый корень — общую папку, в которой находятся ярлыки к локальным и удаленным общим

папкам. Пользователям, таким образом, достаточно при использовании системы DFS помнить всего лишь один путь к общей папке, через которую они получают доступ ко всем папкам, которые им нужны.

Эту главную функцию системы DFS мы и используем. Впоследствии мы реализуем и дальнейшие возможности, коими являются автоматическая репликация содержимого между двумя общими папками.

Если вы захотите опробовать это в нашей сети, необходимо сделать следующее:

1. Снова открыть сетевой доступ к папке `Library` на сервере SRVR001.
2. На сервере SRVR002 создать пустую общую папку `Library` и установить для нее такие же разрешения NTFS, как у папки `Library` на компьютере SRVR001.

Далее поступайте следующим образом:

1. Зарегистрируйтесь на SRVR002 как администратор.
2. Запустите утилиту **Распределенная файловая система DFS**. Эта утилита устанавливается при установке операционной системы, и удалить ее невозможно.
3. В окне консоли щелкните правой кнопкой мыши по значку **Распределенная система файлов DFS (Distributed File System)** и из контекстного меню выберите команду **Создать корень**. Запустится Мастер создания нового корня. Нажмите **Далее**.
4. В диалоговом окне **Тип корня** выберите **Доменный корень** и нажмите **Далее**.

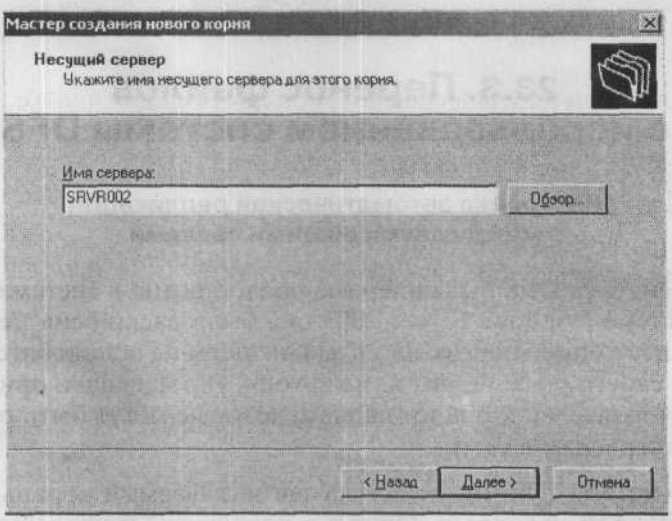


Рис. 23.3. *Сервер SRVR002 будет управлять доменным корнем DFS*

5. В диалоговом окне **Несущий домен** оставьте предложенное значение — домен `study.local` и нажмите **Далее**.
6. В диалоговом окне **Название сервера** введите название сервера, который будет управлять корнем системы DFS (SRVR002). Продолжайте нажатием кнопки **Далее**.
7. В диалоговом окне **Имя для корня** введите имя корневой папки (DFS), UNC-путь к ней (`\\study.local\DFS`) и произвольный комментарий. После этого нажмите **Далее**. Если отобразится сообщение о том, что папка не существует, в поле **Общая папка** введите путь C:\DFS и нажмите **Далее**. Подтвердите свои действия нажатием кнопки **Да**.

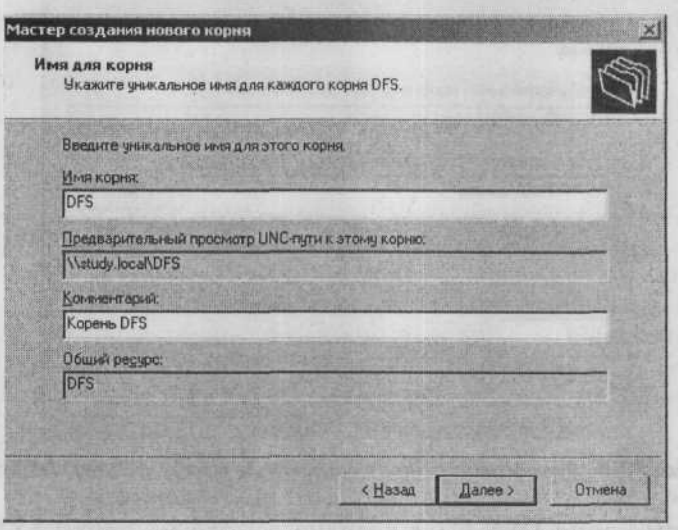


Рис. 23.4. *Параметры корневой папки DFS*

8. В диалоговом окне **Завершение мастера создания нового корня DFS** ещё раз просмотрите введённую информацию и нажмите **Готово**. В консоли **Распределенная файловая система DFS** отобразится новый корень.

Примечание.

В системе Windows Server 2003 вы бы могли создать несколько доменных корней. Возможности системы Windows 2000 ограничиваются одним корнем.

Настройка новой ссылки

Ссылкой DFS в системе Windows Server 2003 называется ярлык к сетевой папке. Создадим ссылку на папку `Library`, находящуюся на сервере SRVR001:

1. В консоли **Распределенная файловая система DFS** щелкните правой кнопкой мыши по значку доменного корня и из контекстного меню выберите команду **Создать ссылку**.
2. Заполните поле в диалоговом окне **Новая ссылка** по рисунку 23.5. Изучите путь, указанный в поле **Предварительный просмотр UNC –пути к ссылке**. Продолжите нажатием на **OK**.

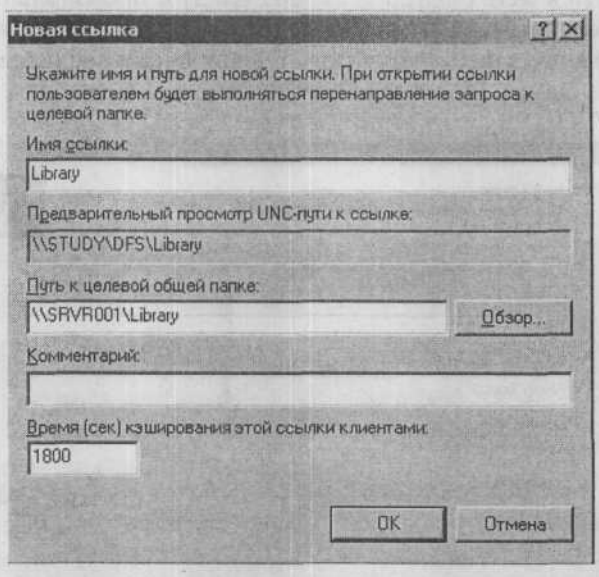


Рис. 23.5. *Диалоговое окно со ссылкой на папку \\SRVR001\Library*

В доменном корне DFS была создана ссылка на папку `\\SRVR001\Library`. По стечению обстоятельств эта ссылка также носит название «Library», хотя это не является обязательным. Существенным является и тот факт, что пользователи могут теперь получить доступ к документам при помощи пути `\\study.local\DFS\Library`.

Может, вам покажется несколько странным использовать в UNC-пути имя домена вместо имени компьютера, но это выгодно тем, что позволяет в дальнейшем переместить корневую папку на другой компьютер незаметно для пользователей.

Что изменится для пользователей

Теперь у вас появилось достаточно времени для того, чтобы научить пользователей использовать вместо UNC-пути `\\SRVR001\Library` путь `\\study.local\DFS\Library`. Несмотря на то, что первый путь до сих пор активен, желательно, чтобы пользователи привыкли к новому пути, который не зависит от имени компьютера.

После того, как пользователи полностью перейдут на использование нового UNC-пути, мы можем продолжать перемещать библиотеку на сервер SRVR002.

Примечание.

Системы Windows 9X/ME/NT не могут использовать систему DFS.

23.4. Репликация библиотеки на сервер SRVR002

23.4.1. Последовательность действий по репликации

После того, как пользователи начнут использовать UNC-путь системы DFS, необходимо, чтобы вы хорошо спланировали перенос структуры таким образом, чтобы для пользователей папка `Library` целиком находилась на одном компьютере. Система DFS не умеет разрешать конфликты и в случае доступности обеих реплик (копий) одной папки перенаправляет одних пользователей на один сервер, а других — на другой, выравнивая таким образом нагрузку. Это может привести к ошибкам, если два пользователя откроют в хранилище один и тот же файл, причём каждый — на своём сервере.

Понятие реплики в консоли DFS отображается как **Цель**. Добавим к существующей ссылке ещё одну цель — папку `Library` на сервере SRVR002. Поступайте следующим образом:

1. В консоли **Распределенная файловая система DFS** щелкните правой кнопкой мыши по ссылке `Library` и из контекстного меню выберите команду **Создать целевую папку**.
2. В диалоговом окне **Новая целевая папка** задайте в поле **Путь к общей целевой папке** путь `SRVR002\\Library`. Флажок **Добавить эту целевую папку к набору репликации** оставьте установленным и нажмите **OK**.
3. Отобразится вопрос, нужно ли настроить репликацию: ответьте **Да**. Если вопрос не отобразится или если вы по ошибке нажали **Нет**, выберите из контекстного меню ссылке `Library` команду **Настроить репликацию**. Запустится Мастер настройки репликации. Нажмите **Далее**.
4. В следующем диалоговом окне Мастера выберите пункт `SRVR001\Library` и нажмите кнопку **Промежуточное хранение**. Откроется

диалоговое окно **Промежуточная папка**, в котором вы можете в поле **Промежуточная папка** задать локальную папку (например, `C:\DFS-Temp`). Нажмите **ОК** и укажите ту же промежуточную папку для другой целевой папки на компьютере SRVR002.

5. Потом выберите из списка `SRVR001\Library` и нажмите **Далее**. Вы определили, что первая репликация произойдёт из папки `Library` на сервере SRVR001 в папку `Library` на сервере SRVR002. Обратный порядок мог бы иметь нежелательные последствия.
6. В диалоговом окне с выбором топологии оставьте исходные параметры и нажмите **Готово**.

В течение 15 минут должна произойти репликация папки `Library` на компьютер SRVR002. Для первой репликации необходимо указать ее направление (с какого сервера на какой), а для последующих репликаций этого делать не нужно. Это значит, что изменение файла на любом из серверов будет скопировано (реплицировано) на все остальные цели. Это свойство мы можем очень просто проверить:

1. В одной из папок библиотеки документов на компьютере SRVR001 создайте какой-нибудь файл.
2. Откройте ту же папку на компьютере SRVR002 и проверьте, что новый файл появился (подвергся репликации).
3. Следующий новый файл создайте в одной из папок библиотеки на компьютере SRVR002.
4. Проверьте, что файл подвергся репликации на компьютер SRVR001.

Эту возможность мы использовать не собираемся именно потому, что система DFS не умеет разрешать конфликты: единственной версией файла она считает последнюю по времени сохранения. Поэтому после завершения начальной репликации удалите целевую папку `SRVR001\Library` из распределенной файловой системы DFS.

23.4.2. Остановка репликации и удаление первоначальной папки из репликации

1. В левой части консоли **Распределенная файловая система DFS** щелкните правой кнопкой мыши по ссылке `Library` и из контекстного меню выберите команду **Остановить репликацию**. Подтвердите нажатием **Да**.
2. В правом подокне щелкните правой кнопкой мыши по объекту `SRVR001\Library` и из контекстного меню выберите команду **Удалить целевую папку**.
3. Отобразится запрос на подтверждение удаления. Нажмите **Да**.

Если теперь пользователь введет UNC-путь в виде `\\study.local\DFS\Library`, то отобразится папка, расположенная на сервере SRVR002. Не все пользователи, однако, уже привыкли к новому пути, и может найтись пользователь, который по привычке попробует путь `\\SRVR001\Library`. Этот пользователь попадет в устаревшую папку на сервере SRVR001. Чтобы он потом не удивлялся, почему никто не обращает внимания на его исправления в документах, запретите доступ к устаревшей папке.

23.4.3. Закрытие доступа к папке на сервере SRVR001

Для закрытия доступа к папке на исходном сервере SRVR001:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Запустите Проводник и перейдите к диску C:.
3. Отобразите свойства папки `Library`, перейдите на вкладку **Доступ** и снимите флажок разрешения сетевого доступа.
4. Можете совсем удалить папку `Library`.

Система DFS проделала массу работы автоматически. Она перенесла на SRVR002 содержимое всех подпапок хранилища документов со всеми их разрешениями и атрибутами. В то же время она предоставляет возможность использовать доступ к файлам через UNC-путь, не зависящий от конкретного компьютера.

Эта система имеет и свои минусы по сравнению с предыдущим (ручным) способом переноса. Она не умеет подвергать репликации зашифрованные файлы и в течение репликации (особенно начальной) создает огромный трафик в сети. Невозможность репликации зашифрованных файлов в хранилище документов нам не слишком мешает, поскольку при его создании мы запретили шифровать общие файлы (вспомните файл DESKTOP.INI).

Чтобы мы полностью использовали возможности службы DFS, необходимо дополнить информацию о сохранении созданного доменного корня. Его мы создали на компьютере SRVR002 в папке DFS. Если в сети установлена система DFS, обычно в ней создаются также ссылки на все сетевые папки. Предположим, что мы хотим добавить DFS-ссылку на папку `Протоколы`, предоставленную в общий доступ с компьютера SRVR001.

1. В консоли **Распределенная файловая система DFS** щелкните правой кнопкой мыши по корню (`study.local\DFS`) и из контекстного меню выберите команду **Создать ссылку**. Откроется диалоговое окно **Новая ссылка**.

2. Поля в диалоговом окне **Новая ссылка** заполните согласно рис. 23.5, только вместо имени папки `Library` укажите `Протоколы`. Нажмите кнопку **OK**.
3. С любого компьютера проверьте доступ к папке `Протоколы` по UNC-пути `\\study.local\DFS\Протоколы`.

Несмотря на то, что файловая система DFS значительно упрощает доступ пользователям к общим файлам (поскольку пользователи не обязаны помнить, какой компьютер открыл общий доступ к какой папке), в нашей сети существует в эту минуту слабое место, от которого зависит работа системы DFS. Это слабое место — корень DFS. Не объект корня как таковой, который записан в базе данных Active Directory, но папка, в которой содержатся отдельные ссылки. В нашем случае — папка DFS на компьютере SRVR002.

Если SRVR002 выйдет из строя, то доступ через ссылки DFS не будет работать. Конечно, адресация через имена компьютеров (например, `\\SRVR001\Протоколы`) работать по-прежнему будут, но пользователи-то к тому времени забудут эти имена.

Выходом из этой ситуации будет репликация корня на еще один компьютер с серверной операционной системой Windows 2000/2003. Поступайте следующим образом:

1. В консоли **Распределенная файловая система DFS** щелкните правой кнопкой мыши по корню (`study.local\DFS`) и из контекстного меню выберите команду **Создать целевую корневую папку**.
2. В диалоговом окне **Несущий сервер** в поле **Имя сервера** введите SRVR001 и нажмите **Далее**.
3. В диалоговом окне **Корневая общая папка** в поле **Путь к целевой общей папке** введите путь `C:\DFS` (обычно путь, в котором будет сохранена реплика DFS). Продолжайте нажатием кнопки **Далее**.
4. Если заданная папка не существует, отобразится сообщение с предложением её создать. Нажмите **Да**.
5. В диалоговом окне **Завершение мастера добавления коренного адресата** просмотрите заданные параметры и нажмите **Готово**. В консоли отобразится новая реплика (цель) DFS.
6. На компьютере SRVR001 откройте папку `C:\DFS` и убедитесь, что без настройки какой-либо репликации произошло копирование ссылок в корневую папку DFS с компьютера SRVR002.

Этим шагом мы исключили возможность недоступности сетевых папок в случае поломки компьютера SRVR002. Если у вас есть возможность, выключите компьютер SRVR002 и потом попробуйте с любой рабочей станции открыть сетевую папку по ее DFS-ссылке, начинающейся со `\\study.local`.

23.5. Дальнейшие рекомендуемые шаги

После перенесения документов на другой файловый сервер и установки службы DFS ещё далеко не всё готово. На исходном компьютере существовали еще другие параметры, которые влияли на возможности пользователей, но автоматически они перенесены не были. После переноса файлов хорошо будет сделать следующее:

- **Теневое копирование.** Если вы перенесли хранилище документов на диск C:, не забудьте настроить теневое копирование этого раздела. Тем самым вы обеспечите пользователям доступ к предыдущим версиям документов, который может понадобиться в случае ошибочного изменения или удаления файла.
- **Настройка автоматической архивации.** Нужно архивировать файловый сервер. Однако, чтобы вам не приходилось всё время об архивации думать, лучше всего настроить архивационные задания для автозапуска. Дальнейшая информация о стратегиях архивации и конфигурации автоматической архивации находится в главе 16.
- **Настройка дисковых квот.** На сервере SRVR001 мы настроили дисковые квоты при помощи объекта групповой политики по имени «Disk quotas», который применяется к организационной единице Domain Controllers. Нет смысла перемещать учётную запись рядового сервера SRVR002 в эту организационную единицу. Нужно связать объект «Disk quotas» с той организационной единицей, в которой находится SRVR002, или применить фильтрацию объектов групповой политики (глава 17). В крайнем случае можно настроить квоты локально — прямо в свойствах дисковых разделов на SRVR002.

23.6. Итоги

Если вы собираетесь установить в сети еще один сервер, переложив на него те обязанности, которые чрезмерно перегружают контроллер домена, то необходимо учесть возможности оборудования нового сервера.

Перенос файлов следует тщательно спланировать. Пользователи не должны лишиться данных и прав доступа к файлам с учетом дополнительных атрибутов (шифровки, сжатия) и после переноса должны быть способны работать с ними.

Существует несколько вариантов переноса. Если вы будете переносить данные вручную, самым разумным будет использовать механизм архивации системы (NTBackup.exe). Вы тем самым обеспечите безопасное перенесение всех атрибутов. Если вы будете копировать или перемещать файлы, вы можете потерять разрешения NTFS, атрибуты сжатия и шиф-

рования. Более того, право копировать или перемещать зашифрованные файлы имеет только их хозяин, причём нужно помнить, что зашифрованные файлы перед переносом дешифруются. Единственным безопасным способом переноса зашифрованных файлов будет использование утилиты архивации.

Альтернативным решением переноса будет использование распределенной файловой системы DFS. Она изначально предназначена для облегчения доступа к сетевым папкам и делает возможным также автоматическую репликацию корня и содержимого конкретных файлов. Её использование для переноса содержимого общих папок — только малая часть ее возможностей. Зашифрованные файлы она реплицировать не умеет, разрешать конфликты тоже.

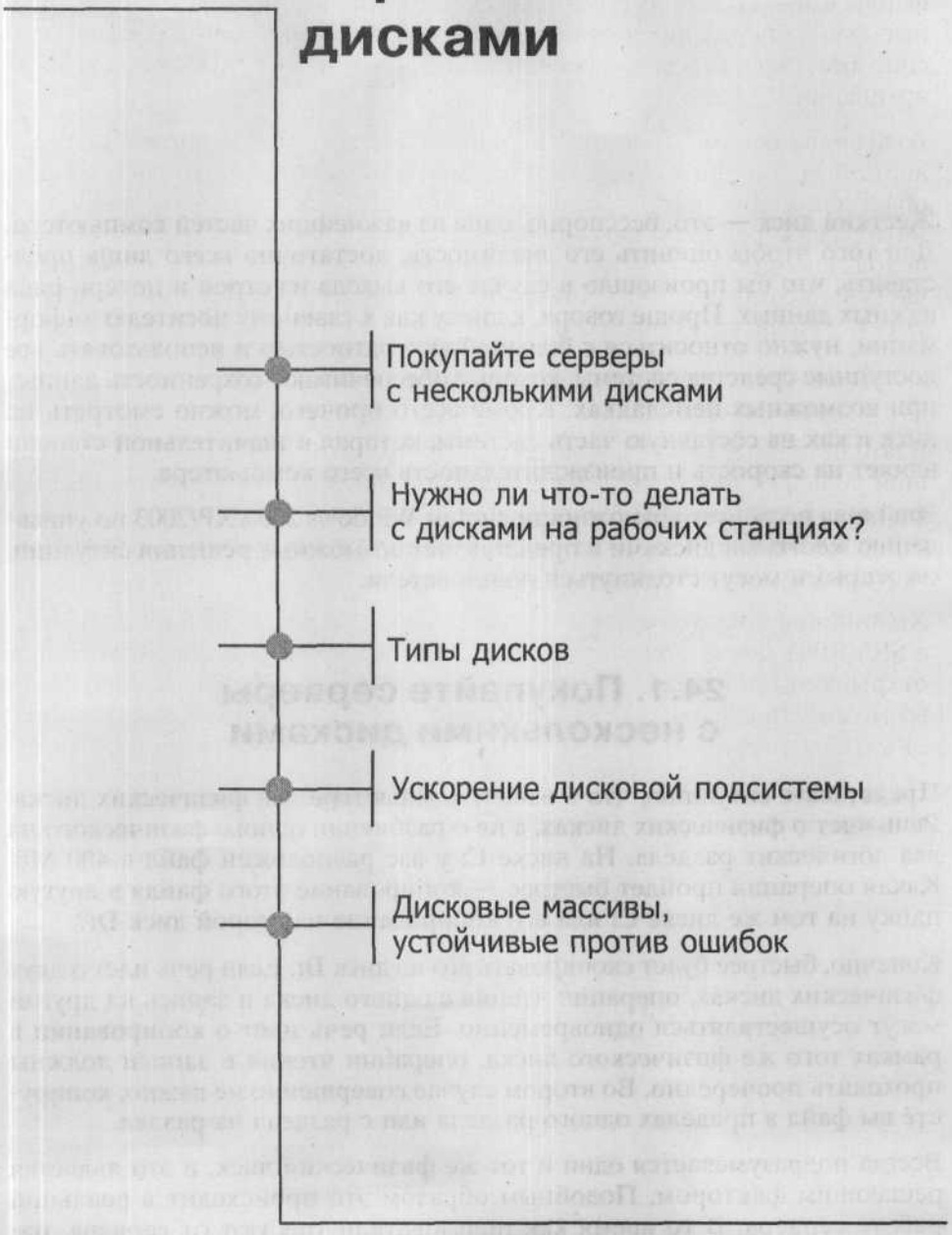
Состояние сети

В домен `study.local` добавлен новый компьютер SRVR002, выполняющий роль файлового сервера. Создан доменный корень распределенной файловой системы DFS. Его реплики находятся в папках `C:\DFS` на серверах SRVR001 и SRVR002 и таким образом делают некритичным выход из строя сервера SRVR002.

Хранилище документов предприятия перенесено на сервер SRVR002, а с SRVR001 после этого все файлы были удалены. Пользователи теперь открывают библиотеку не по пути `\\SRVR002\Library`, а используют возможности системы DFS и указывают путь в формате `\\study.local\DFS\Library`.

На сервере SRVR002 настроена регулярная архивация, теневое копирование и дисковые квоты раздела C:.

Глава 24 Управление дисками



Жесткий диск — это, бесспорно, одна из важнейших частей компьютера. Для того чтобы оценить его значимость, достаточно всего лишь представить, что бы произошло в случае его выхода из строя и потери ряда важных данных. Проще говоря, к диску как к главному носителю информации, нужно относиться с большой аккуратностью и использовать все доступные средства системы, которые обеспечивают сохранность данных при возможных неполадках. Кроме всего прочего, можно смотреть на диск и как на составную часть системы, которая в значительной степени влияет на скорость и производительность всего компьютера.

Эта глава исследует возможности систем Windows 2000/XP/2003 по управлению жесткими дисками и представляет возможные решения ситуаций, с которыми могут столкнуться пользователи.

24.1. Покупайте серверы с несколькими дисками

Представьте ситуацию, что в вашем компьютере два физических диска. Речь идет о физических дисках, а не о разбиении одного физического на два логических раздела. На диске **C:** у вас расположен файл в 400 Мб. Какая операция пройдет быстрее — копирование этого файла в другую папку на том же диске **C:** или его копирование на второй диск **D:**?

Конечно, быстрее будет скопировать его на диск **D:**. Если речь идет о двух физических дисках, операции чтения с одного диска и запись на другой могут осуществляться одновременно. Если речь идет о копировании в рамках того же физического диска, операции чтения и записи должны проходить поочередно. Во втором случае совершенно не важно, копируете вы файл в пределах одного раздела или с раздела на раздел.

Всегда подразумевается один и тот же физический диск, и это является решающим фактором. Подобным образом это происходит в реальной работе сервера. В то время как пользователи требуют от сервера, например, обработать вызов базы данных, сервер считывает и размещает системные файлы, данные приложений, базу данных, содержимое памяти, выгруженное в файл подкачки и т. п.

Теперь вы определенно ощущаете, что если все эти файлы находятся на одном физическом диске, то это, с точки зрения производительности, худшее из возможных решений. Самый простой шаг, который вы можете сделать для повышения производительности сервера, это добавить дисков.

24.1.1. Сколько дисков должно быть на сервере?

Сперва необходимо отметить, что однозначного ответа на этот вопрос не существует.

В целом к серверам применяются следующие правила:

- Файл подкачки должен быть отделен от системных файлов.
- Файлы приложений должны быть отделены от системных файлов.
- Данные приложений должны быть отделены от файлов приложений.
- База данных приложений и системных служб должна быть отделена от журналов этих приложений и служб.

Остальные файлы размещаются отдельно по необходимости.

Что же сервер SRVR001? В соответствии с приведенными правилами можете назначить его дискам следующие функции (таблица 24.1).

Назначение физических дисков сервера SRVR001 *Таблица 24.1*

Диск	Назначение
C:	Операционная система
D:	Файл подкачки
E:	Файлы службы Удаленной установки
F:	Двоичные файлы приложений
G:	База данных Active Directory
H:	Протоколы базы данных Active Directory
I:	Разделяемые папки
J:	Очередь печати

Назначение физических дисков сервера SRVR002 приведено в таблице 24.2.

Назначение физических дисков сервера SRVR002 *Таблица 24.2*

Диск	**Назначение**
C:	Операционная система
D:	Файл подкачки
E:	Файлы файлового сервера

Сервер SRVR001 не является специальным сервером и, несмотря на это, должен был бы содержать 7 дисков? Возможно ли вообще подключить к

нему столько дисков? Не всегда. Поэтому встает вопрос об оптимизации количества дисков, то есть отступлении от оптимального решения под давлением физических возможностей сервера с одной стороны и финансовых возможностей предприятия — с другой. Результатом может быть, например, следующее разделение дисков сервера SRVR001 (таблица 24.3).

Назначение имеющихся физических дисков сервера SRVR001 *Таблица 24.3*

Диск	Назначение
C:	Операционная система, двоичные файлы приложений, база данных Active Directory
D:	Файл подкачки
E:	Файлы службы Удаленной установки, очередь печати, разделяемые папки, протоколы базы данных Active Directory

Некоторые данные можно перенести легко. Другие нужно инсталлировать (например, приложения), а некоторые требуют использования специальных настроек.

24.1.2. Перенос файла подкачки

Файл подкачки не является стандартным файлом, от содержимого которого зависит работоспособность системы. Это всего лишь место хранения данных, которые были загружены в оперативную память компьютера, но в данный момент не используются. В целях безопасности можно настроить групповые политики так, чтобы при выключении компьютера этот файл уничтожался, а при включении создавался заново.

Файл подкачки нельзя перемещать как обычный файл. Перенос файла подкачки означает вмешательство в функционирование операционной системы. Перенос на диск **D:** можно осуществить следующим способом:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. В меню **Пуск** или на рабочем столе щелкните правой кнопкой мыши по значку **Мой компьютер** и из контекстного меню выберите команду **Свойства**.
3. В диалоговом окне **Свойства системы** перейдите на вкладку **Дополнительно** и там в части **Быстродействие** нажмите на кнопку **Параметры**. Появится диалоговое окно **Параметры быстродействия**.
4. Перейдите на вкладку **Дополнительно** и в области **Виртуальная память** нажмите кнопку **Изменить**. Появится диалоговое окно **Виртуальная память**.
5. Выберите из списка диск **D:** и поставьте переключатель в положение **Особый размер**. В поле **Исходный размер (Мб)** введите величину файла подкачки, равную или в полтора раза превышающую размер

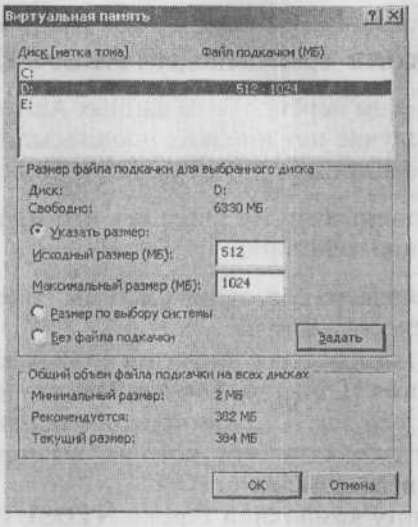


Рис. 24.1. *Настройка файла подкачки (виртуальной памяти)*

оперативной памяти, в поле **Максимальный размер (Мб)** введите удвоенную величину оперативной памяти.

6. Нажмите кнопку **Задать**. Заданный размер файла подкачки появится в верхней части окна.
7. Потом выберите диск **C:** и поставьте переключатель в положение **Без файла подкачки**. Нажмите кнопку **Задать**. Может появиться окно предупреждения о возможной ошибке при загрузке. Ответьте утвердительно на вопрос о применении параметра.
8. Щелкнув на кнопке **OK**, закройте диалоговое окно **Виртуальная память**.

Вы можете также, отметив **Размер по выбору системы**, поручить принятие решения о размере файла подкачки операционной системе.

Примечание редактора.

Не рекомендуется использовать этот режим, т. к. он требует от системы отслеживать необходимый размер файла, что будет отнимать процессорное время.

В некоторых случаях при определении размера файла подкачки будет уместным использовать одинаковые величины в поле **Исходный размер** и в поле **Максимальный размер**. Если файл подкачки достигнет большего размера, чем исходный, система должна его увеличить. Для этого, однако, потребуется процессорное время и система некоторое время будет занята. Если вы зададите одинаковые величины, системе не нужно будет увеличивать файл подкачки и эта проблема не возникнет.

24.1.3. Перенос базы данных и протокола транзакций Active Directory

В этой части мы покажем перенос базы данных Active Directory на другой диск, хотя в нашем случае нет никаких предпосылок к этому действию. Подобным же образом происходит перенос протоколов транзакций.

При переносе базы данных Active Directory или протоколов транзакций выполняйте следующие действия:

1. Проведите архивацию состояния системы контроллера домена, где вы будете переносить файлы.
2. Перезагрузите компьютер и запустите его в режиме **Восстановления службы каталогов** (Directory Services Restore Mode).
3. Зарегистрируйтесь как Администратор с паролем для режима восстановления службы каталогов, который вы определили при инсталляции контроллера домена.
4. Запустите утилиту командной строки **NTDSUTIL**.
5. Введите команду FILES, чтобы перейти в режим **File Maintenance**.
6. Если вы хотите перенести протоколы операций базы данных Active Directory, введите команду `move logs to e:\ntds`. Произойдет перенос протоколов.
7. Если вы хотите перенести базу данных Active Directory, введите в режиме File Maintenance команду `move db to` путь, где путь представляет собой место для размещения базы данных Active Directory.
8. Введите команду **INFO** и убедитесь, что протоколы перенесены в нужные места.
9. Два раза подряд введите команду **quit**, чтобы вернуться в обычную командную строку.
10. Перезагрузите компьютер.

Сразу после перезагрузки компьютера вам следует провести архивацию, потому что, если через несколько часов вам придется восстанавливать систему из архивной копии, то протоколы базы данных (или сама база данных) вернутся на прежнее место.

24.2. Нужно ли что-то делать с дисками на рабочих станциях?

Рабочие станции — это, как правило, обычные компьютеры, не обладающие широкими возможностями. Исключение могут составлять, например, графические рабочие станции, в которых наличие нескольких дисков, несомненно, найдет себе применение.

Обычные станции, с точки зрения быстродействия, не имеют больших требований к дисковой подсистеме, и одного диска будет достаточно. В предыдущих главах мы перенесли на серверы почти все данные пользователя, включая профили. На жестких дисках клиентских компьютеров, таким образом, остались только файлы операционной системы и двоичные файлы приложений.

В следующих параграфах мы посмотрим на возможности оптимизации дисков у высокопроизводительных рабочих станций и на решение проблем с пользователями, которые обязательно потребуют добавить свободного места на уже заполненном диске.

Речь пойдет о так называемых динамических дисках.

24.3. Типы дисков

Системы Windows 2000/XP/2003 могут работать с двумя типами дисков. Первый тип — это так называемые обычные диски. Эти диски отличаются ограничениями, которые уже сегодня могут в некоторых случаях мешать разумной работе. Решением данной проблемы является преобразование в динамические диски, у которых нет ограничений, свойственных обычным дискам, однако они применимы только к системам Windows 2000 и более новым.

24.3.1. Обычные диски

Обычные диски хранят свою конфигурацию в так называемых таблицах размещения файлов (Master File Table, MFT). В этой таблице может быть не более четырех записей — каждая запись соответствует разделу.

Разделы подразделяются на первичные и расширенные. Первичный раздел соответствует одному логическому диску, а расширенный раздел может содержать несколько логических дисков. Логические диски именуются буквами английского алфавита.

Главным ограничением обычных дисков является как раз количество разделов и невозможность создавать более сложные структуры, которые, например, могли бы увеличить быстродействие компьютера. Однако, с другой стороны, большинство рабочих станций клиентов инсталлируется с одним диском, разбитым на два раздела, и это ограничение не играет большой роли.

24.3.2. Динамические диски

Динамические диски — это лучшее решение в том случае, если при использовании обычных дисков вы столкнетесь с их ограничениями. Так как речь идет о новом типе дисков, они не совместимы с системами более старыми, чем Windows 2000. Это не означает, что остальные системы в сети не смогут с ними общаться (это определяют другие службы); динамические диски невозможно будет использовать в операционных системах, установленных на этом же компьютере (система с двойной или множественной загрузкой).

Динамические диски могут использовать как клиентские, так и серверные операционные системы.

24.4. Ускорение дисковой подсистемы

Предположим, что в компьютере, кроме системного диска, на котором установлена Windows Server 2003, есть еще два физических диска. Если диски будут в компьютере уже с самой инсталляции операционной системы, они будут сразу отображены в консоли **Управление дисками**. Если вы вставите в компьютер диски только после инсталляции операционной системы, при первом запуске консоли **Управление дисками** запустится Мастер подключения новых дисков (рис. 24.2). Нажмите **Далее**.

1. В диалоговом окне **Выбор диска для инициализации** оставьте отмеченными все диски, которые вы хотите добавить в систему, и нажмите **Далее**.

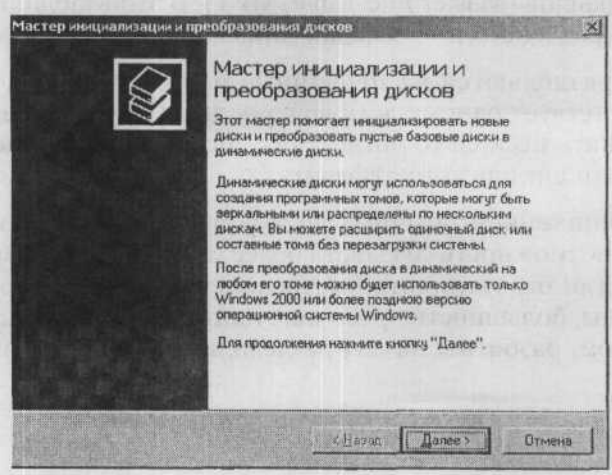


Рис. 24.2. *Мастер инициализации и преобразований дисков*

2. В диалоговом окне **Выбор дисков для преобразования** не отмечайте ничего и сразу нажмите **Далее**. Преобразование дисков мы проведем позже.
3. Нажмите **Готово**. Новые диски теперь отобразятся в консоли **Управление дисками**.

На компьютер под управлением Windows XP Professional новые диски устанавливаются точно так же.

Преобразование дисков в динамические

Только что добавленные диски преобразуем в динамические. Это условие дальнейшей возможности работы с дисками. С первым физическим диском, содержащим инсталляцию операционной системы, этого сделать не удастся, поэтому оставим его как обычный диск. Перед преобразованием не рекомендуется создавать на дисках другие разделы. Выполните следующие действия:

1. В консоли **Управление дисками** щелкните правой кнопкой мыши по кнопке того физического диска, который вы хотите преобразовать в динамический (рис. 24.3) и из контекстного меню выберите команду **Преобразовать в динамический диск**.

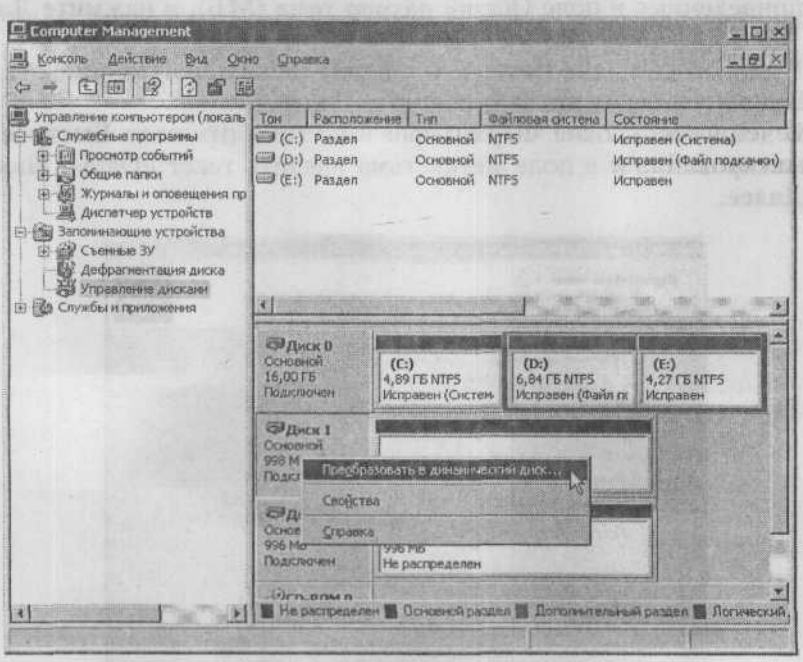


Рис. 24.3. *Для преобразования диска в динамический нужно щелкнуть мышью в довольно неожиданном месте*

2. В диалоговом окне **Преобразовать в динамический диск** отметьте **Диск 1** и **Диск 2** и нажмите **ОК**.
3. Произойдет преобразование дисков в динамические. Если в этот момент не был открыт никакой файл, компьютер не будет требовать перезагрузки.
4. У преобразованных дисков теперь в консоли **Управление дисками** есть отметка **Динамический**.

Эти два диска будут теперь использоваться для размещения информации. Чтобы работа с данными, насколько это возможно, ускорилась, создадим так называемый чередующийся том величиной в 1 Гб.

1. В консоли **Управление дисками** щелкните правой кнопкой мыши по любому месту на диске и из контекстного меню выберите команду **Создать том**. Появится Мастер создания тома. Нажмите **Далее**.
2. В диалоговом окне **Выбрать тип тома** есть больше возможностей. Однако нас будет интересовать **Чередующийся том** (рис. 24.4). Установите переключатель в это положение и нажмите **Далее**.
3. В диалоговом окне **Выбор дисков** отметьте в левой части **Диск 2** и, нажав кнопку **Добавить**, присоедините его к тем дискам, которые уже есть в этом томе. В поле **Выберите размер выделяемого пространства (МБ)** введите число 500. Обратите внимание на величины, приведенные в поле **Общий размер тома (МБ)**, и нажмите **Далее**.
   Рис. 24.5. *Определение дисков, которые станут составной частью тома*
4. В диалоговом окне **Назначение буквы диска или пути** оставьте предложенную букву диска и нажмите **Далее**.
5. В диалоговом окне **Форматирование тома** отметьте **Быстрое форматирование** и в поле **метка тома** введите текст «Data». Нажмите **Далее**.

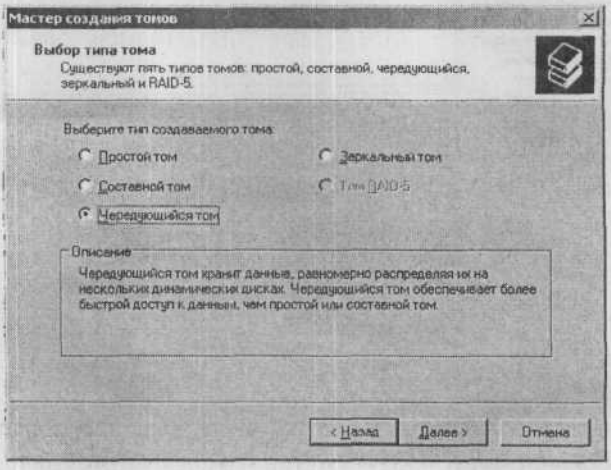


Рис. 24.4. *Определение чередующегося тома*

6. В последнем диалоговом окне просмотрите заданную информацию и нажмите **Готово**.
7. Теперь на обоих дисках появились разделы одинаковой величины, образующие *Чередующийся том*. Диск **E:** теперь готов к использованию.

Как работает чередующийся том?

Если пользователь, например, разместит на диске **E:** файл размером в 1 Мб, это будет выглядеть следующим образом.

Первые 64 Кб файла разместятся на первом диске (**Диск 1**). Вторые 64 Кб — на втором диске (**Диск 2**). Следующие 64 Кб разместятся опять на первом диске, следующие — опять на втором и т. д. Так как информация одновременно пишется на два диска, этот процесс происходит намного быстрее, чем обычная последовательная запись на один диск. То же самое относится и к считыванию. Величину блока данных, равную 64 Кб, нельзя изменить.

Если один из дисков, составляющих чередующийся том, выйдет из строя, пользователь потеряет все данные. Чередующийся том — это только способ ускорения процесса записи и считывания информации с диска, однако если вы решитесь его использовать, позаботьтесь о постоянном дублировании информации, которая на нем размещена.

Упрощение работы пользователей

В этом параграфе мы покажем, как пользователи, которые привыкли записывать информацию только на один том, могут создать дальнейшее пространство для записи.

Следующая последовательность может быть использована только в том случае, когда:

1. Пользователь хранит свои данные не на системном диске (обычно это диск **C:**).
2. Диск, на котором пользователь хранит данные, преобразован в динамический еще до создания раздела, который использует пользователь.

Чтобы смоделировать это состояние, создадим на **Диске 1** другой том размером в 100 Мб. Том создайте согласно предыдущим указаниям со следующими изменениями:

- В пункте 2 выберите **Простой том**;
- В пункте 3 оставьте отмеченным только **Диск 1**, а в поле **Выберите размер выделяемого пространства (МБ)** введите число 100.

- Теперь пользователь имеет для записи 100 Мб свободного места на томе **F:**, которое когда-нибудь закончится. Что делать потом?

Расширение тома

Если вы на динамическом диске, все очень просто — вы можете расширить том. Условием для этого будет использование на расширяемом диске файловой системы NTFS. Действуйте согласно следующим указаниям:

1. Правой кнопкой мыши щелкните по значку диска **F:** и из контекстного меню выберите команду **Расширить том**. Запустится Мастер расширения тома. Продолжайте, нажав кнопку **Далее**.
2. В диалоговом окне **Выбор дисков** введите в поле **Выберите размер выделяемого пространства (МБ)** число, на которое вы хотите расширить том (например, 50 Мб). В поле **Общий размер тома (МБ)** потом появится сумма текущего размера и заданной величины. Нажмите **Далее**.
3. В последнем диалоговом окне нажмите **Готово**.

Если вы теперь посмотрите на состав дисков в консоли **Управление дисками**, вы увидите, что расширенное место здесь отмечено как новый том. Однако учтите, что это изменение откатить назад не удастся. Если в контекстном меню вы выберете команду **Удалить том**, то будет удален весь том и пользователь лишится своих данных. Расширение томов, таким образом, нужно хорошо планировать. Разумеется, теперь не составит труда расширять том дальше и дальше.

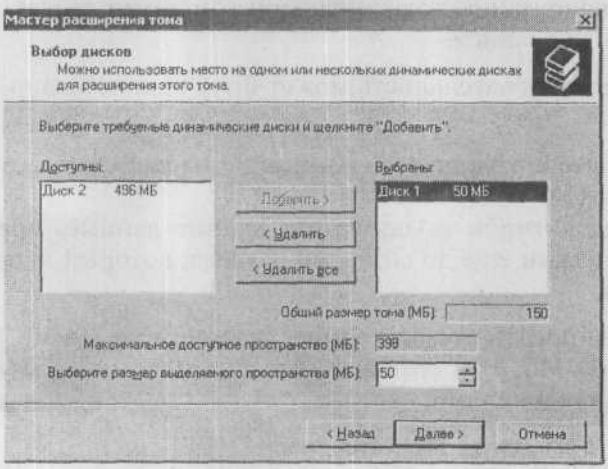


Рис. 24.6. *При расширении тома введите число мегабайт, на которое вы хотите его расширить*

Если вам будет нужно расширить том, а на диске, где он сейчас расположен, уже недостаточно места, вы можете выбрать для расширения другой динамический диск. В этом случае создайте так называемый **Составной том.**

Создание составного тома проводится так же, как и расширение существующего тома, с тем отличием, что в диалоговом окне **Выбор диска** в левой части списка **Выбранные:** будет указан другой динамический диск.

Составной том вы можете создать сразу, не обязательно в тот момент, когда на исходном диске закончится место. Выбор только за вами. Однако будьте осторожны, так может произойти утрата информации, как и в случае с чередующимся томом, если один из дисков, входящих в составной том, выйдет из строя.

Промежуточные итоги

Хорошо известно, что клиентские операционные системы могут работать с динамическими дисками. В некоторых случаях эта возможность может сильно пригодиться. На практике использование динамических дисков, однако, имеет смысл только на специализированных рабочих станциях, на которых установлено несколько физических дисков. В подавляющем большинстве случаев эта функция на клиентских компьютерах не используется.

Преобразование дисков в динамические нужно очень хорошо планировать, так как если вы хотите вернуться к обычным дискам, нужно провести архивацию всех данных, удалить с диска все тома и потом таким же способом, как и при преобразовании в динамический диск, преобразовать в обычный.

24.5. Дисковые массивы, устойчивые против ошибок

Что станет с сервером, если из строя выйдет системный диск? Можем ли мы вообще допустить такую ситуацию? Можно ли к ней подготовиться?

Ответ относительно прост. Это возможно, но требует знаний и достаточного количества жестких дисков.

В начале этой главы была приведена информация о том, как должно выглядеть оптимальное расположение информации на жестких дисках. Что если бы мы добавили, что лучше всего было бы все удвоить?

Если в вашем распоряжении есть достаточное количество дисков, которые можно подключить к конкретному серверу, не составит никаких проблем создать такие тома, которые справятся с выходом из строя одного физического диска. Безусловно, здесь предполагается, что одновременно не выйдет из строя больше чем один диск.

Поломка большего числа дисков опять бы означала выход из строя всего сервера. К томам, которые могут справиться с поломкой одного диска, относится так называемый RAID-массив (сокращение от Redundant Array of Independent Disks) типа 1 или 5.

24.5.1. RAID-1, или зеркальный том

Принцип зеркального массива очень прост — вся информация будет дублироваться. В случае выхода из строя одного из дисков необходимая информация будет предоставлена другим. Для реализации этого принципа вам понадобится:

- Система Windows Server 2003 или Windows 2000 Server.
- Два динамических диска.

В случае программной реализации зеркального тома нет ограничения на идентичность дисков. Если зеркалирование дисков реализовано аппаратно, то диски обязаны быть одинаковыми.

Что защищать?

Обычно рекомендуется использовать зеркалирование для системных и загрузочных томов. Системный том — это тот, в котором расположены загрузочные файлы, загрузочный том — тот, в котором инсталлирована система Windows. Запутанно, не правда ли? В большинстве случаев оба названия относятся к одному и тому же диску **C:**.

Как работает зеркалирование

За процесс дублирования информации в системах Windows Server 2003 и Windows 2000 отвечает файл `FTDISK.SYS` (FT = Fault Tolerant, т.е. «устойчивый к ошибкам»). Это драйвер, заботящийся о том, чтобы при записи данные писались на оба диска синхронно. Рассинхронизация данных при зеркалировании недопустима.

При считывании данных с диска драйвер `FTDISK.SYS` читает с основного диска и переключается на другой только при ошибке чтения с основного.

Настройка зеркального тома

Зеркальный том — это разновидность составного тома, слегка отличающаяся от него порядком настройки.

Предположим, что мы собираемся дублировать системный раздел **C:**. Нам понадобится новый диск размера не меньшего, чем диск **C:**.

Поступайте следующим образом:

1. Запустите консоль **Управление дисками** и проверьте, являются ли оба диска (системный и новый) динамическими. Если нет, преобразуйте их. Так как вы преобразуете системный диск, компьютер нужно будет перезагрузить.
2. После перезагрузки снова запустите консоль **Управление дисками**.
3. Правой кнопкой мыши щелкните по значку диска **C:** и из контекстного меню выберите команду **Добавить зеркало**.
4. Появится диалоговое окно **Добавить зеркальный том**. Отметьте диск, на который вы хотите отразить системный диск, и потом щелкните на кнопке **Добавить зеркальный том**.
5. Система создаст зеркальный том и проведет копирование данных (синхронизацию). Это может продолжаться несколько минут.

После проведения синхронизации можно сказать, что жесткий диск застрахован от поломки, однако не на сто процентов. Может случиться, что после выхода из строя главного жесткого диска (диска **C:**) произойдет перезагрузка компьютера и будет необходимо его запустить со второго

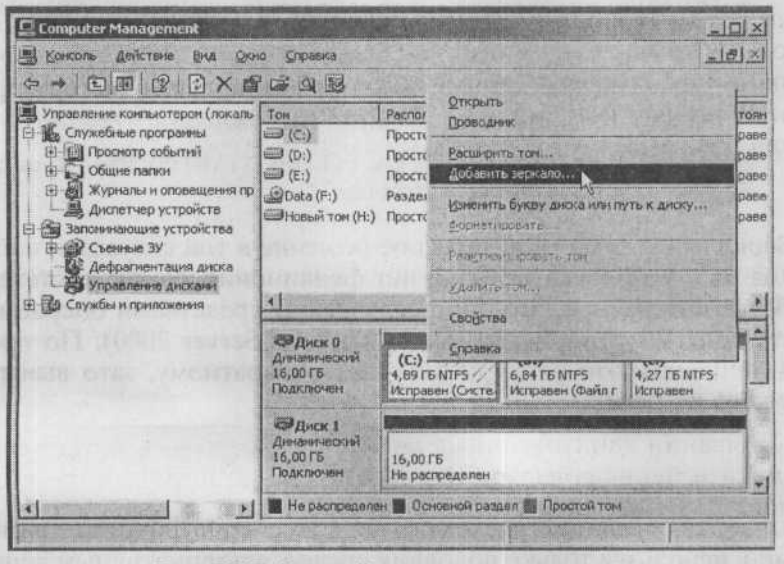


Рис. 24.7. *Настройка зеркального массива*

диска. Для этого, однако, нужно, чтобы существовала запись в файле `BOOT.INI` (в противном случае не будет обнаружена операционная система).

Для создания записи в файле `BOOT.INI` выполните следующие действия:

1. В меню **Пуск** или на рабочем столе щелкните правой кнопкой мыши по значку **Мой компьютер** и откройте его свойства.
2. На вкладке **Дополнительно** в части **Загрузка и восстановление системы** нажмите кнопку **Параметры**. Появится диалоговое окно **Загрузка и восстановление системы**. Нажмите кнопку **Правка**. Откроется приложение **Блокнот**, и в нем отобразится этот файл.
3. Убедитесь, что в пункте `[operating systems]` существует не менее двух записей (если в компьютере одна система). В нашем случае здесь существует следующая строчка:

```
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows
Server 2003, Standard"/fastdetect
```

Эта запись означает, что операционная система будет загружаться из папки Windows, которая находится в первом элементе (partition(1)) на первом жестком диске (rdisk(0)), присоединенном к первому каналу контроллера (multi(0)). Теперь многое зависит от способа присоединения второго диска. Если он будет присоединен к тому же контроллеру, будет нужно в этом файле добавить следующую строчку:

```
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows
Server 2003, Standard(mirror)"
```

Если бы другой жесткий диск был присоединен как мастер к другому контроллеру IDE, строка выглядела бы так:

```
multi(1)disk(0)rdisk(0)partition(1)\WINDOWS="Windows
Server 2003, Standard(mirror)"
```

Зеркальные тома — интересное решение в той ситуации, когда выход из строя диска не угрожает функционированию системы. Тем более интересное, что они реализованы средствами операционной системы Windows Server 2003 (Windows Server 2000). По производительности это решение уступает аппаратному, зато выигрывает у него по цене.

24.5.2. RAID-5

Так как зеркалирование расходует дисковое пространство крайне неэкономно, используя только половину дисков, альтернативным решением

может стать том RAID-5 (чередующийся массив с контрольной суммой). Он тоже реализован средствами серверных операционных систем Windows Server 2003 и Windows 2000 Server.

Для настройки тома RAID 5 должны быть выполнены следующие условия:

- Операционная система Windows Server 2003 или Windows 2000 Server;
- Не меньше трех (максимум 32) динамических дисков.

Для чего использовать RAID 5

В массиве RAID-5 не может участвовать системный или загрузочный диск. Этот массив предназначен для хранения пользовательских данных, но ни в коем случае не данных операционной системы. Массив RAID 5 устанавливается в систему как единый том.

Как работает том RAID-5

Представьте себе 3 жестких диска, на которых созданы разделы одинаковой величины (диски не обязательно должны быть одинаковой величины). При записи файла на том RAID-5 первые 64 Кб запишутся на первый жесткий диск, а другие 64 Кб — на второй диск.

На третий диск будет записана контрольная сумма — цепочка данных, полученная из порций данных, уложенных на первый и второй диски. При выходе первого диска из строя блок данных, потерянный на нем, можно будет восстановить по контрольной сумме и блоку данных на втором диске.

При записи следующих 128 Кб положение порций данных смещается: первый блок записывается на второй диск, второй блок — на третий диск, а контрольная сумма — на первый. И так по кругу. В результате при выходе из строя любого диска по двум оставшимся дискам можно восстановить весь файл.

Из принципа работы тома RAID-5 видны и его недостатки — медленные запись и считывание данных. При реализации RAID-5 средствами операционной системы Windows вам придется с этим смириться.

Настройка тома RAID 5

Для успешной настройки тома RAID 5 вам понадобится как минимум три жестких динамических диска (не считая системного). Если они есть у вас в компьютере, действуйте согласно следующим указаниям:

1. В консоли **Управление дисками** щелкните правой кнопкой мыши на любом месте любого из трех жестких дисков (на нем уже может быть создан раздел) и из контекстного меню выберите команду **Создать том**. Запустится Мастер создания тома. Продолжите нажатием кнопки **Далее**.
2. В диалоговом окне **Выбор типа тома** отметьте RAID 5 и нажмите **Далее**.

Примечание.

Если элемент RAID 5 неактивен, значит, у вас нет трех динамических дисков или вы работаете не в серверной операционной системе.

3. В диалоговом окне **Выбор дисков** добавьте в список **Выбранные** хотя бы три жестких диска. В поле **Выберите размер места (МБ)** автоматически добавится свободное место — минимум из всех выбранных дисков. Его размер может только уменьшаться, но никак не увеличиваться. Обратите внимание на используемую величину в поле **Общий размер тома (МБ)** и нажмите **Далее**.
4. В диалоговом окне **Назначение буквы диска или пути** оставьте изначальные настройки и нажмите **Далее**.
5. В диалоговом окне **Форматировать том** выделите **Быстрое форматирование**, введите описательный текст в поле **Метка тома** и нажмите **Далее**.
6. В диалоговом окне **Завершение работы мастера создания тома** просмотрите заданные параметры и нажмите **Готово**.
7. После создания и форматирования тома пройдет синхронизация содержимого и после этого том будет готов к использованию в полном объеме.

24.6. Итоги

Дисковая подсистема — одна из важнейших составных частей, которые влияют на всю работу системы. Чтобы справиться с недостаточной производительностью компьютера, в некоторых случаях можно добавить еще дисков и перенести некоторые части системы или приложения.

Системы Windows 2000/XP/2003 работают с двумя видами дисков — с обычными и динамическими. Если при работе с обычными дисками нельзя ожидать никаких широких возможностей, то с динамическими дисками можно конфигурировать следующие тома:

- Простые
- Составные

- Чередующиеся
- Зеркальные
- RAID-5

Первые три типа томов есть во всех системах, зеркальные тома и тома RAID-5 — только в серверных системах.

На рабочих станциях специальные тома имеют особое значение только в особых случаях, когда нужно ускорить дисковую подсистему или добавить пользователям еще свободного места с помощью расширения действующих дисков.

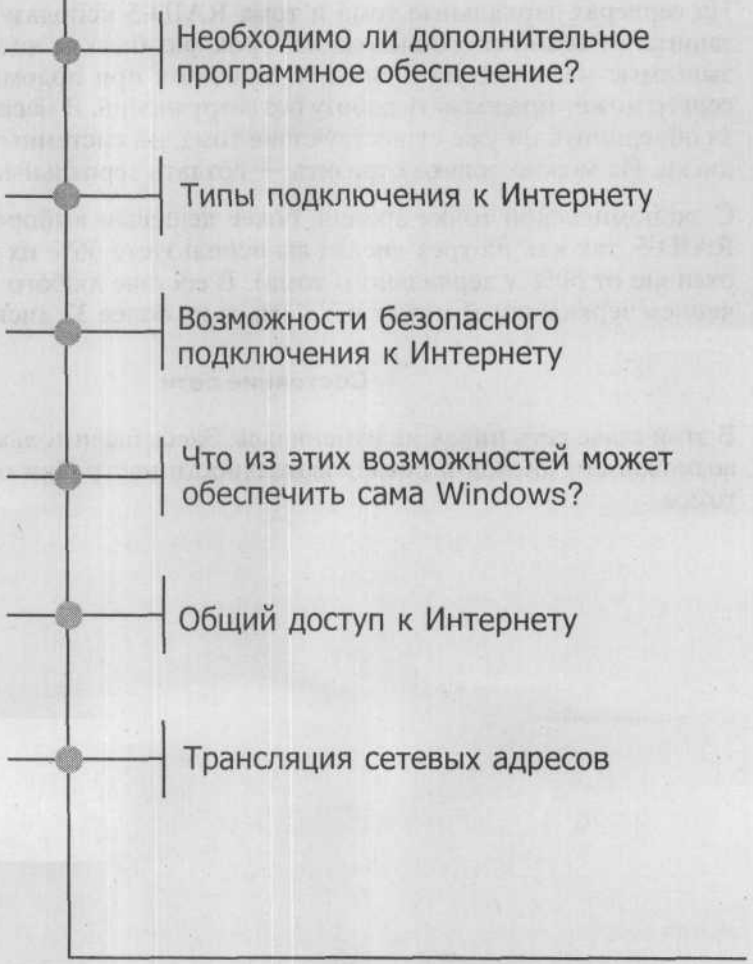
На серверах зеркальные тома и тома RAID-5 используются в качестве защиты от возможного выхода из строя физических дисков. Это так называемые массивы, устойчивые к ошибкам: при поломке одного диска сервер может продолжать работу без затруднений. В массив RAID-5 нельзя объединить ни уже существующие тома, ни системный и загрузочный диски. Их можно только отразить — создать зеркальный том.

С экономической точки зрения, более дешевым выбором является том RAID-5, так как на трех дисках вы используете 66% их пространства (в отличие от 50% у зеркального тома). В составе любого тома (за исключением зеркального) может находиться не более 32 дисков.

Состояние сети

В этой главе сеть никак не изменилась. Здесь были только представлены возможности дисков и последовательности настройки отдельных типов томов.

Глава 25 Соединяем локальную сеть с Интернетом



Дискуссия о том, стоит ли соединять сеть с Интернетом, не имеет смысла. При помощи Интернета коммуникации между компаниями становятся проще, дешевле и, прежде всего, быстрее. Пользователи, а главное, администраторы имеют под рукой достаточно информации, которая им необходима для работы, а компании получают недорогую возможность публиковать свои предложения или продавать свою продукцию через электронные магазины.

Однако Интернет также хранит в себе и угрозы для нашей сети (речь идет о сети, в которой все компьютеры могут соединяться друг с другом). Надо помнить, что далеко не все пользователи имеют чистые помыслы. Не надо забывать и о таких вещах, как вирусы. Они появляются не сами, их делают люди и люди же распространяют. Так или иначе, достоинства Интернета преобладают над его недостатками.

Эта часть главы описывает действия, при помощи которых вы сможете соединить свою сеть с Интернетом без больших финансовых затрат и очень просто.

25.1. Необходимо ли дополнительное программное обеспечение?

Когда на практике говорят о сетях и их соединении с Интернетом, большинство администраторов и пользователей использует слово «прокси» (Proxy). Что, собственно, такое этот «прокси»? Действительно ли он необходим?

Слово «прокси» в переводе с английского означает «заместитель, посредник, доверенный». Применительно к компьютерной технике и сетям употребляется обозначение «прокси-сервер».

Если в сети для подключения к Интернету используется прокси-сервер, это означает, что клиентские компьютеры не соединяются с Интернетом напрямую, а используют посредника для этого подключения. Например, пользователь хочет подключиться к веб-странице компании Microsoft по адресу `http://www.microsoft.ru`. Он запросит об этом подключении прокси-сервер, который при помощи специального программного обеспечения сохранит запрос клиента и затем попытается установить соединение с сервером, на котором расположена веб-страница `http://www.microsoft.ru`.

Если такое соединение установить удастся, прокси-сервер передаст ответ исходному компьютеру, пославшему запрос. Если же он настроен соответствующим образом, то прокси-сервер еще и сохранит полученную информацию в своей кэш-памяти; это делается на тот случай, если другой компьютер в ближайшее время запросит информацию с той же страницы. Соединение, таким образом, будет более быстрым (компьютер получит информацию с прокси-сервера) и не будет впустую тратить трафик на скачивание данных из Интернета.

Таким образом, прокси-сервер является не просто соединительным звеном между компьютером-клиентом и Интернетом, он служит также и временным хранилищем для скачанных файлов. Есть еще ряд задач, с которыми он может справиться. Для пользователей и менее опытных администраторов в момент, когда речь заходит о подключении к Интернету, прокси-сервер является практически единственным решением. Остается только выбрать какой-то из них, купить лицензию — и вперед, к установке и настройке.

Подключение к Интернету необходимо разделить на две части -- возможность вообще подключиться и безопасность доступа.

25.2. Типы подключения к Интернету

Типы подключения, определяемые прокси-сервером, часто бывают неточными. В принципе, существуют два варианта, которые различаются тем, видна или нет внутренняя сеть предприятия извне.

- **Подключение при помощи маршрутизатора.** В этом случае каждый компьютер во внутренней сети независим и должен иметь собственный IP-адрес. Соединение с компьютерами в Интернете обеспечивается маршрутизатором.

Недостатков у такого способа сразу несколько. Первый — необходимость иметь публичный IP-адрес для идентификации в сети каждого компьютера. Аренда такого адреса стоит денег, и чем больше у предприятия компьютеров, тем за большее количество адресов ему придется платить. Следующим недостатком является сложность управления всей средой. Каждый клиентский компьютер в сети виден из Интернета, и это повышает требования к обеспечению безопасности.

- **Соединение с помощью службы трансляции сетевых адресов.** Трансляция сетевых адресов (Network Address Translation, NAT) отличается использованием приватных IP-адресов и сокрытием от внешнего мира всей локальной сети за исключением единственного компьютера, обладающего единственным публичным IP-адресом. Из Интернета, таким образом, невозможно напрямую связаться с каким-либо компьютером в сети, пространство сети является более защищенным и простым в управлении.

25.3. Возможности безопасного подключения к Интернету

Способы защиты делятся на:

- **Фильтрация портов.** Если некто извне по вашему публичному IP-адресу будет запрашивать, например, веб-службу, вы можете запретить доступ к этой службе, запретив прием пакетов на порт 80 протокола TCP. Данные, направленные извне на этот порт, никогда не дойдут до локальной сети.
  Единственный веб-сервер, который вы можете использовать, должен быть размещен вне вашей сети.
- **Фильтрация по приложениям на уровне протокола IP.** Этот сравнительно новый способ фильтрации применяется все чаще. Если в вашей сети имеется веб-сервер, к которому возможен доступ извне, то вы можете просматривать тип доступа по протоколу IP. Можно задать правила, которые пропустят только трафик, адресованный конкретным веб-приложениям, а остальные пакеты будут отклонены.

25.4. Что из этих возможностей может обеспечить сама Windows?

Возможно, это покажется удивительным, но все описанные возможности подключения можно реализовать средствами систем Windows Server 2003 и Windows Server 2000.

Эти операционные системы можно настроить как маршрутизаторы. Тем не менее, для подключения к Интернету с использованием публичного IP-адреса и учетом необходимости защиты эта возможность используется очень редко. Однако это не говорит о том, что системы Windows Server 2003/Windows 2000 Server совсем не используются как маршрутизаторы.

Гораздо более частым вариантом обеспечения соединения с Интернетом при помощи систем Windows Server 2003 является трансляция сетевых адресов (NAT). С ней Windows Server 2003 справляется без затруднений, и ее настройка наиболее проста. В наличии имеются, опять-таки, две возможности настройки, которые зависят от конкретной сети и требований предприятия.

В области обеспечения защиты доступа к сети из Интернета система Windows Server 2003 способна лишь обеспечить фильтрацию портов, и то с ограничениями. Для фильтрации приложений на уровне протокола IP нужно устанавливать дополнительное программное обеспечение. Лучше всего подходит ISA Server 2000, превосходящий аналогичные продукты по соотношению цена/качество.

В дальнейшем мы рассмотрим возможности подключения сети к Интернету и фильтрацию трафика. Вместе с этим будем предполагать, что постоянное соединение с Интернетом осуществляется при помощи стандартного сетевого адаптера.

Примечание редактора.

Подключением к Интернету должен заниматься администратор, но в любом случае монтаж внешнего оборудования будет производить сторонняя организация. Так что вы будете отвечать за участок до сетевого адаптера вашего сервера.

25.5. Общий доступ к Интернету

Общий доступ к Интернету (Internet Connection Sharing) в точности соответствует своему названию. Он позволяет компьютерам совместно использовать существующее подключение. Один из компьютеров является центральным, он и подключен к Интернету, и это подключение необходимо разделить с остальными компьютерами.

Способностью организовать общий доступ к сети Интернет (не путать с общим доступом к модему) располагают все системы Windows 2000/XP/2003, в том числе клиентские. То есть вы можете организовать общее подключение через обычную рабочую станцию, если ее режим работы и загруженность другими заданиями это позволяют.

Подключение к Интернету зависит не только от собственно самого подключения, в игру вступают также другие службы, которые должны работать в сети. Речь, разумеется, идет о службе DNS и о службе DHCP, раздающей IP-адреса, необходимые для подключения к Интернету клиентских компьютеров.

Произведем настройку службы **Общий доступ к подключению Интернет** в нашей сети. Категорически не рекомендуется выходить в Интернет через тот же сервер, который выполняет роль сервера DNS или контроллера домена. В нашей сети обе роли выполняет компьютер SRVR001, так что настраивать общий доступ к Интернету мы будем на сервере SRVR002.

25.5.1. Предварительная подготовка

Готовимся

Предварительная подготовка состоит из следующих этапов:

1. Установите на компьютере SRVR002 еще один сетевой адаптер.
2. Зарегистрируйтесь на SRVR002 как администратор и откройте окно **Сетевое окружение.**
3. Так как перед этим был установлен еще один сетевой адаптер, в сетевом окружении появится еще один элемент с именем «Подключение по локальной сети 2». Для лучшей ориентации переименуем оба подключения следующим образом:

   «Подключение по локальной сети → «LAN»
   «Подключение по локальной сети 2» → «Internet»

4. В свойствах подключения к Интернету настройте параметры протокола IP в соответствии с информацией, предоставленной провайдером.

Примечание.

Если вы всего лишь проверяете эти действия вне сети (режим тестирования), настройте IP-адрес, например, на значение 200.200.200.200 с маской подсети 255.255.255.240. IP-адрес сервера DNS не настраивайте.

Теперь необходимо проверить, что IP-адрес для соединения с Интернетом верный. Без каких-либо дополнительных настроек вы должны получить доступ к ресурсам Интернета с локального компьютера (сайты и файлы).

Правильный порядок сетевых подключений

Если на компьютере установлено несколько сетевых адаптеров, необходимо установить правильный порядок их использования. Так как в доменах Active Directory не обойтись без службы DNS и поскольку адреса серверов DNS настраиваются в свойствах протокола IP, неправильный порядок сетевых адаптеров в серверах может вызвать ситуацию, в которой не будут применяться объекты групповой политики, могут появиться сложности, увеличится время входа в систему и запуска приложений. Поэтому порядок сетевых адаптеров необходимо проверить и, если нужно, исправить:

1. Зарегистрируйтесь на SRVR002 как администратор.
2. Откройте окно **Сетевые подключения** и на вкладке **Дополнительно** нажмите кнопку **Дополнительные параметры**. Откроется диалоговое окно **Дополнительные параметры**, в котором можно настроить порядок привязки подключений.
3. На вкладке **Адаптеры и привязки** убедитесь в том, что в поле **Подключения** на первом месте находится сетевой адаптер LAN, а далее следуют все остальные адаптеры (Интернета и, возможно, другие).
4. Нажатием на кнопки со стрелками в правой части диалогового окна можно изменить не устраивающий вас порядок.
5. Нажатием на кнопку **OK** подтвердите изменения и закройте диалоговое окно.

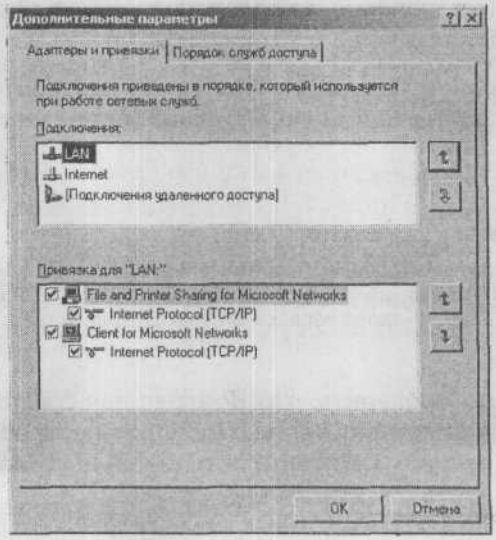


Рис. 25.1. *Диалоговое окно порядка привязок*

Примечание.

Если в консоли **Просмотр событий** обнаружится несколько сообщений об ошибках, касающихся невозможности применить объекты групповой политики (безотносительно к настройке общего доступа к Интернету), обязательно проверьте порядок привязок. В большинстве случаев причина ошибок заключается именно в этом.

25.5.2. Настройка общего доступа к Интернету

Для настройки общего доступа сделайте следующее:

1. Зарегистрируйтесь на SRVR002 как администратор и отобразите свойства подключения к Интернету (сетевого подключения, только что переименованного в «Internet»).
2. На вкладке **Дополнительно** отметьте в части **Общий доступ к подключению к Интернету** поле **Разрешить другим пользователям сети использовать подключение к Интернету этого компьютера.**
3. Нажмите на кнопку **ОК.** Появится сообщение, приведенное на рисунке 25.3. Просто согласитесь с предложенным IP-адресом, нажав кнопку **Да.**

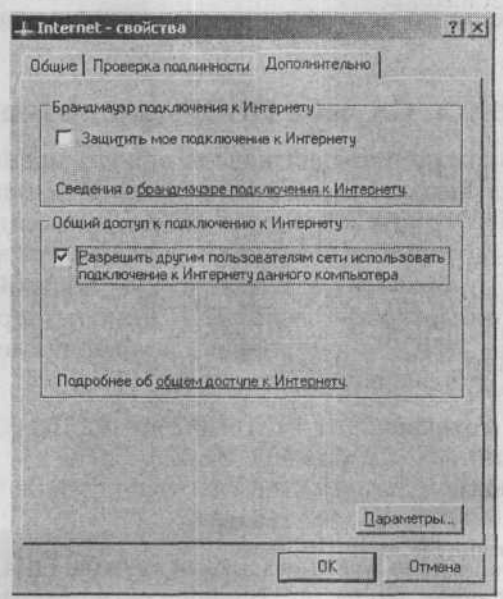


Рис. 25.2. *Вкладка Дополнительно в диалоговом окне* ***Свойства подключения к Интернету***

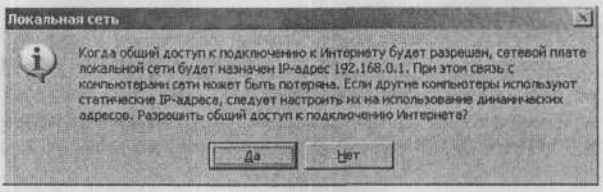


Рис. 25.3. *Информация о необходимости изменения IP-адреса сетевого адаптера в локальной сети*

25.5.3. Как работает общий доступ?

Для указанной функции в системах Windows выделена подсеть 192.168.0.0/24. Для того чтобы общий доступ начал работать, в уведомлении о смене IP-адреса необходимо нажать кнопку **Да**.

Сетевой адаптер локальной сети будет настроен на адрес 192.168.0.1 с маской подсети 255.255.255.0 (заметьте, что о маске подсети нигде не упоминается) и общий доступ к Интернету будет разрешен. Для того, чтобы все это работало, клиентские компьютеры, которые хотят получить доступ к Интернету, должны иметь «подобный» адрес и для них должна быть настроена служба DNS, которая будет преобразовывать имена в Интернете.

Служба общего доступа к Интернету самостоятельно обеспечивает все функции для успешного подключения всех компьютеров.

25.5.4. Служба DHCP-диспетчер

Служба DHCP-диспетчер предназначена для упрощения настройки рабочих станций для подключения к Интернету. Поскольку такой способ подключения к Интернету определен скорее для одноранговых сетей (peer-to-peer), для которых не характерно наличие сервера DHCP, служба DHCP-диспетчер производит автоматическую настройку IP-протокола на клиентских компьютерах. Служба DHCP-диспетчер является, таким образом, сервером DHCP с настроенными значениями, которые невозможно изменить. Эти значения следующие:

- Диапазон IP адресов: от 192.168.0.2 до 192.168.0.254
- Маска подсети: 255.255.255.0
- Основной шлюз: 192.168.0.1
- DNS сервер: 192.168.0.1

Если в сети на самом деле нет стандартной службы DHCP, все в порядке. Однако в нашем случае это не так. В нашей сети помимо службы DHCP-диспетчер, имеется также сервер DHCP, и клиентские компьютеры скорее получат IP-адрес от него. Однако это может вызвать серьезную нагрузку

на сеть. Стандартный сервер DHCP сейчас выделяет IP-адреса из подсети 192.168.10.0/24, с которых клиентские компьютеры не подключатся к Интернету, а если полностью перейти на службу DHCP-диспетчер, то клиентские компьютеры будут иметь неправильный адрес сервера DNS и не смогут корректно работать в локальной сети.

Для нашей сети имеется единственное решение, которое заключается в ручной настройке клиентских компьютеров. Другим способом нельзя разрешить конфликт в выделении адресов сервера DNS. Если для вашей сети это так, действуйте согласно следующим инструкциям:

1. Зарегистрируйтесь на SRVR001 как администратор.
2. Запустите консоль DHCP и деактивируйте настроенную область.
3. Отобразите свойства подключения к локальной сети и настройте параметры протокола IP следующим образом: IP-адрес 192.168.0.2, маска подсети 255.255.255.0, основной шлюз 192.168.0.1, адрес DNS-сервера 192.168.0.2 (должен быть клиентом для себя). Если используется сервер WINS, задайте следующее значение его адреса; 192.168.0.2.
4. Поочередно зарегистрируйтесь как администратор на всех клиентских компьютерах и других сетевых устройствах, использующих сервер DHCP, и вручную настройте протокол IP следующим образом:
   - IP-адрес : от 192.168.0.3 до 192.168.0.254
   - Маска подсети: 255.255.255.0
   - Основной шлюз: 192.168.0.1
   - DNS-сервер: 192.168.0.2

При присвоении IP-адреса принимайте во внимание план их распределения, описанный в главе 3, «Учим компьютеры общаться в сети», где мы определили диапазоны IP-адресов, присваиваемых серверам, клиентским компьютерам и сетевому оборудованию. С учетом довольно значительного (глубокого) изменения в настройках целой сети необходимо запланировать изменение IP-адресов на время, когда пользователи не работают на компьютерах.

Поэтому после окончания ручной конфигурации, подключение к Интернету еще не будет работать. Здесь не хватает механизма преобразования имен.

25.5.5. Служба прокси DNS

Поскольку служба общего подключения к Интернету определена преимущественно для сетей peer-to-peer, для которых не характерно наличие сервера DNS, ее компонентой является служба Прокси DNS. Прокси DNS определяет для клиентских компьютеров трансляцию внешних имен, то есть Интернет-имен. Компьютер с разрешенным общим доступом своего

подключения к Интернету работает как ретранслятор, и любые запросы, настроенные на подключение к Интернету, ретранслирует серверу DNS.

Если бы в сети работала только служба DHCP-диспетчер и клиентские компьютеры получали IP-адреса от нее, то можно было бы обойтись без дальнейшей настройки. В нашей сети это, однако, невозможно. Сервером DNS является сервер SRVR001, в то время как подключение к Интернету обеспечивает сервер SRVR002. Если бы все компьютеры использовали как сервер DNS лишь SRVR002, домен Active Directory перестал бы функционировать. Однако этого позволить нельзя, и необходимо обеспечить сосуществование служб DNS и Прокси DNS.

Вся приведенная выше настройка протокола IP на компьютерах говорит о том, что сервером DNS и в дальнейшем будет являться сервер SRVR001. Для успешной трансляции имен Интернета в настоящий момент существует два решения. Первое из них представлено на рисунке 25.4.

Пользователь запрашивает веб-страницу, находящуюся по адресу www.microsoft.com. Первым делом нужно определить IP-адрес, соответствующий имени www в зоне microsoft.com, поэтому рабочая станция отправляет DNS-запрос своему DNS-серверу, которым является компьютер SRVR001. Тот не располагает о зоне microsoft.com никакой информацией и передает запрос на исполнение компьютеру SRVR002.

Компьютер SRVR002, который настроен как Прокси-сервер DNS, передаст запрос на исполнение Интернет-серверу DNS, IP-адрес которого

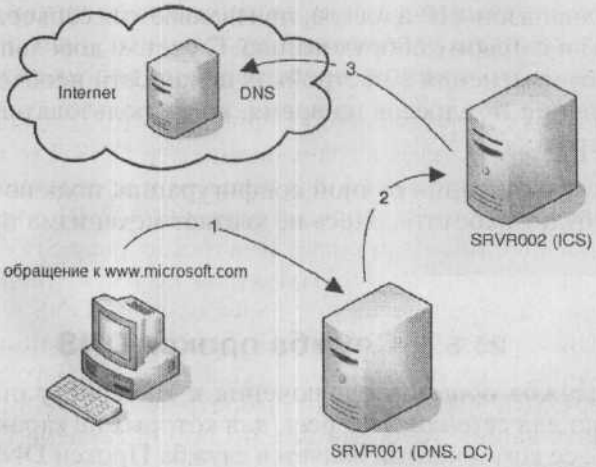


Рис. 25.4. *Запросы DNS, которые не может выполнить сервер SRVR001, передаются на SRVR002*

введён в параметрах подключения к Интернету. После преобразования имени IP-адрес вернётся на рабочую станцию тем же путем, но в обратном порядке.

Для того чтобы приведенная последовательность работала, на сервере SRVR001 необходимо настроить перевод невыполненных запросов DNS серверу SRVR002. Это можно сделать согласно следующим инструкциям:

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль DNS.
2. Правой кнопкой мыши щелкните по серверу SRVR001 и из контекстного меню выберите команду **Свойства.**
3. В диалоговом окне **SRVR001 — Свойства** перейдите на вкладку **Пересылка.** Убедитесь в том, что в части **Домен DNS** присутствует запись **Все остальные домены DNS**, а в поле **Список IP-адресов серверов пересылки для данного домена** сервера для выбранного домена введите IP-адрес локального сетевого адаптера компьютера SRVR002. Затем нажмите кнопку **Добавить.**
4. Нажатием на кнопку **OK** подтвердите произведенные изменения и закройте диалоговое окно.

Приведенная настройка сделана для среды, в которой не используется служба DNS и для локального сетевого адаптера не указан DNS-сервер. Такой локальный адаптер любые приходящие запросы автоматически передает внешнему сетевому адаптеру. Если компьютер является членом домена (как в нашем случае), то на его локальном адаптере настроен IP-адрес внутреннего сервера DNS, которому он будет передавать все запросы, и трансляции имен Интернета не будет происходить.

В доменном окружении удобно настроить топологию для трансляции имен несколько иначе (и возможно, проще). Речь идет о втором возможном решении, и его принцип представлен на рисунке 25.5.

Не дайте рисунку запутать себя. Сервер SRVR002 здесь вынесен лишь потому, что он не участвует в трансляции имен DNS. Его нельзя совсем не принимать во внимание, поскольку именно он предоставляет соединение с Интернетом. Если клиент запросит сервер SRVR001 о трансляции имени компьютера в зоне microsoft.com в IP-адрес, сервер SRVR001 попробует выполнить данный запрос. Поскольку он не имеет информации о зоне microsoft.com, то передаст запрос далее серверу DNS в Интернете. Это необязательно должен быть сервер DNS, рекомендованный провайдером (сервер, IP-адрес которого приведен в свойствах сетевого адаптера Internet в компьютере SRVR002). Можно выбрать любой DNS-сервер, который будет отвечать вашим требованиям, но выбор сервера DNS провайдера предпочтителен.

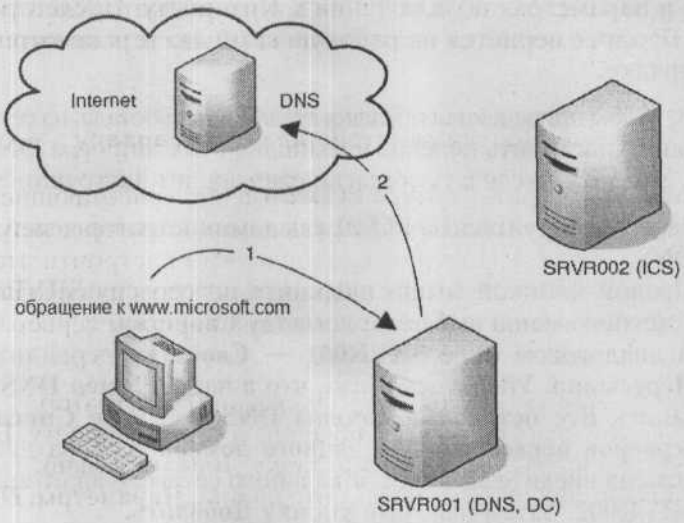


Рис. 25.5. *Трансляция внешних имен DNS в среде домена со службой Общий доступ подключения к Интернету*

25.5.6. Безопасность сети и доступ к ресурсам Интернета

После успешной настройки пользователи всех компьютеров в сети смогут подключаться к Интернету. Их доступ никоим образом не ограничен. Кроме того, они могут использовать любые службы Интернета (www, ftp, smtp и другие). Лишь от пользователей зависит, каким образом они распорядятся своими возможностями. Способов для ограничения доступа вовне (из локальной сети в Интернет) средствами Windows Server 2003 не существует.

Иначе обстоит дело с доступом извне (из Интернета к локальной сети). Вся сеть, с точки зрения пользователя Интернета, скрыта за одним внешним IP-адресом. Если по этому адресу будут запущены службы www, ftp или smtp, то они будут доступны из Интернета. К службам внутренней сети пользователи Интернета доступ получить не смогут.

Примечание.

Если перед любой настройкой доступа к Интернету на данном компьютере имелась работающая веб-служба, то после установки еще одного сетевого адаптера произойдет ее запуск и для него тоже. Следствием этого после подключения сети к Интернету явится неограниченный, а следовательно, никак не защищенный доступ Интернет-пользователей к веб-службам компьютера.

Однако речь идет о начальной конфигурации, которую в системах Windows Server 2003 можно подкорректировать. Далее рассмотрим различные варианты.

Доступ к внутреннему веб-серверу

Если, например, на компьютере PC001 имеются работающие веб-серверы и вы хотите сделать их доступными для всех пользователей, в том числе и для пользователей Интернета, необходимо настроить этот доступ на компьютере SRVR002, который является шлюзом для входа в сеть. Описанные ниже действия называются публикацией веб-сервера. Действуйте согласно следующим инструкциям.

1. Зарегистрируйтесь на SRVR002 как администратор.
2. Отобразите свойства подключения сети к Интернету. В диалоговом окне свойств перейдите на вкладку **Дополнительно.**
3. В правой нижней части нажмите кнопку **Параметры**. Появится диалоговое окно **Дополнительные параметры**.
4. Отметьте поле **Веб-сервер (HTTP)**. Откроется диалоговое окно **Параметры службы**.
5. В поле **Имя или IP-адрес компьютера** введите имя компьютера **PC001** или его IP-адрес. Проще и быстрее ввести IP-адрес.

Примечание.

Веб-серверы всегда должны иметь статический IP-адрес.

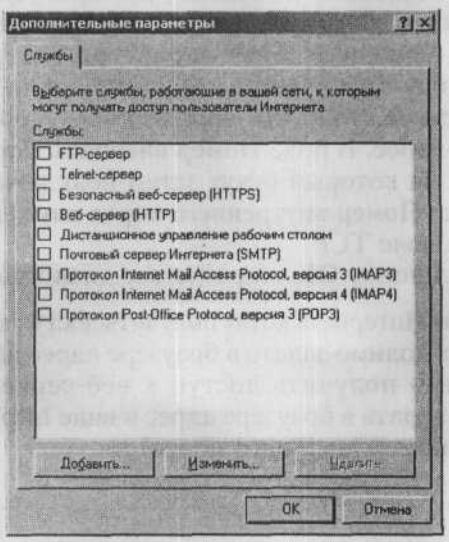


Рис. 25.6. *Диалоговое окно Дополнительные параметры*

6. Заметьте, что для этой службы нельзя исправить номера ни внешнего, ни внутреннего порта и нажатием на кнопку **OK** закройте диалоговое окно.
7. Нажатием на кнопку **OK** закройте остальные открытые диалоговые окна.

Если хотите сделать доступными также и другие службы, отметьте соответствующее поле и произведите конфигурацию аналогично тому, как это было сделано для веб-сервера. Иногда может потребоваться сделать доступным приложение, которое не использует стандартные известные порты. Скажем, речь идет о приложении, использующем порт 880 протокола TCP. В этом случае в диалоговом окне **Дополнительные параметры** нажмите кнопку **Добавить** и в окне **Параметры службы** введите Описание службы, IP-адрес, номера внутреннего и внешнего портов (в обоих случаях 880) и выберите протокол (для TCP).

Иногда может понадобиться организовать доступ к двум внутренним веб-серверам из Интернета. В этом случае возможны два решения. Одно из них предназначено для пользователей, которые знают номер порта, и по нему получают доступ к веб-серверу, второе решение для большой группы пользователей Интернета, которые ожидают, что веб-сервер всегда работает по портам 80 (HTTP) и 443 (HTTPS).

В первом случае поступим следующим образом:

1. Зарегистрируйтесь на SRVR002 как администратор.
2. Отобразите свойства подключения сети к Интернету. В диалоговом окне свойств перейдите на вкладку **Дополнительно**.
3. В правой нижней части нажмите кнопку **Параметры**. Появится диалоговое окно **Дополнительные параметры** (см. рисунок 25.6).
4. Нажмите кнопку **Добавить** и в диалоговом окне **Параметры службы** введите **Описание службы** (например, «веб-сервер на компьютере PC002») и IP-адрес. В поле **Номер внешнего порта службы** введите номер порта, на который будут затем подключаться к веб-серверу извне, а в поле **Номер внутреннего порта службы** введите значение 81 и отметьте поле TCP.
5. Нажатием на кнопку **OK** закройте все диалоговые окна.

Если пользователи из Интернета хотят получить доступ к веб-серверу на компьютере PC001, необходимо задать в браузере адрес http://200.200.200.200. Если же необходимо получить доступ к веб-серверу на компьютере PC002, необходимо задать в браузере адрес в виде http://200.200.200.200:81 (81 здесь означает номер внешнего порта).

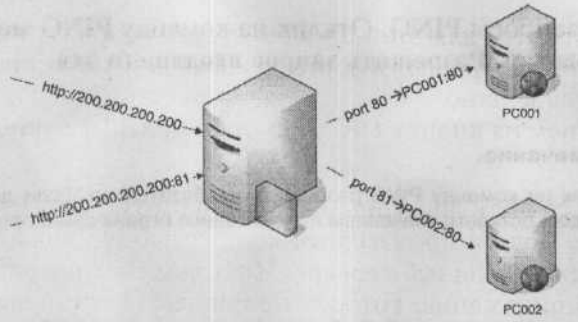


Рис. 25.7. *Доступ к конкретному веб-серверу определяется по номеру порта*

Защита внешнего интерфейса

Операционные системы Windows Server 2003 и Windows XP Professional содержат новую функцию — брандмауэр для защиты подключения к Интернету. Речь идет о блокировании приема внешних пакетов с возможностью настройки исключений.

Конфигурация защиты очень проста:

1. Зарегистрируйтесь на SRVR002 как администратор.
2. Отобразите свойства подключения сети к Интернету. В диалоговом окне свойств перейдите на вкладку **Дополнительно**.
3. В верхней части диалогового окна установите флажок **Защитить мое подключение к Интернету.**
4. Нажатием на кнопку **OK** подтвердите установки и закройте диалоговое окно свойств подключения.

Теперь любое соединение (за исключением настроенных выше) с внешним интерфейсом сети запрещено. Это просто проверить командой PING. На вкладке **Дополнительные параметры** тем временем появятся две новые вкладки — **Ведение журнала безопасности** и **ICMP**.

Если некто извне попытается соединиться с вашей сетью, брандмауэр будет блокировать входящие пакеты. На вкладке **Ведение журнала безопасности** можно определить, нужно ли протоколировать информацию о блокированных пакетах или же успешных подключениях. На этой вкладке можно задать имя, размещение и размер файла протокола.

Вкладка **ICMP** служит для ограничения обмена по протоколу ICMP. Это протокол, по которому устройства, работающие по протоколу TCP, посылают сообщения об ошибках. Утилита **PING** тоже работает по протоколу ICMP. Поскольку в начальной конфигурации брандмауэра все пакеты протокола ICMP запрещены, внешний сетевой адаптер не будет

отвечать на запросы PING. Отклик на команду PING можно разрешить, установив флажок **Разрешить запрос входящего эха**.

Примечание.

Отклик на команду PING разрешать необязательно. Если для этого нет веских доводов, оставьте значением по умолчанию ограничение протокола ICMP.

25.5.7. Итого об Общем доступе к Интернету

Общий доступ к подключению Интернет использует для доступа к Интернету трансляцию сетевых адресов. Этой функцией располагают все системы Windows 2000/XP/2003, в том числе и системы для клиентских компьютеров. Основным ограничением общего доступа к подключению Интернета в больших сетях является необходимость использовать IP-адреса из подсети 192.168.0.0/24. Поскольку изменение IP-адресации является довольно чувствительным вмешательством в сеть, которого некоторые предприятия не могут себе позволить, то на этих предприятиях нужно искать другие способы подключения к Интернету.

Подсеть 192.168.0.0/24 позволяет подключить к Интернету не более 254 компьютеров, в том числе и тот, который обеспечивает это подключение.

Одновременно с разрешением этой функции произойдет автоматический запуск служб DHCP-диспетчер и прокси-сервера DNS. Если в сети используется классический сервер DHCP, он очень плохо сосуществует со службой DHCP-диспетчер, и единственным решением является ручная настройка клиентских компьютеров. Служба прокси DNS будет уже работать без проблем с классической службой DNS. Единственное, что необходимо скорректировать, — это трансляцию внешних имен.

Имея единственный публичный IP-адрес, можно сделать локальные ресурсы (например, веб-сервер) доступными пользователям извне. Это может привести к увеличению загруженности только в случае необходимости сделать доступными большее количество внутренних веб-серверов. Решением в этом случае является использование нестандартных портов протокола TCP, как было показано выше.

25.6. Трансляция сетевых адресов

Трансляция сетевых адресов (Network Address Translation, NAT) является другим решением для подключения сети к Интернету. Она не так ограничена, как вышеприведенный способ, и предоставляет больше

возможностей для настройки. Ее можно использовать лишь в серверных операционных системах (Windows 2000 Server, Windows Server 2003). То есть эта служба является одним из протоколов службы **Маршрутизация и удаленный доступ**.

Этот способ подключения также удобен для нашей сети и обычно используется для любой большой сети с доменной средой.

25.6.1. Основная настройка

Настройку трансляции сетевых адресов произведем на сервере SRVR0-02. Перед этим необходимо удостовериться, что в случае возникновения необходимости возможно будет вернуться к первоначальным значениям. Параметры подключений должны быть следующими:

- **Сервер** SRVR001
  адрес 192.168.10.2
  маска подсети 255.255.255.0
  основной шлюз 192.168.10.1
  адрес сервера DNS 192.168.10.2
  адрес сервера WINS 192.168.10.2
- **Сервер** SRVR002 **(внутренний сетевой адаптер)**
  адрес 192.168.10.1
  маска подсети 255.255.255.0
  адрес сервера DNS 192.168.10.2
  адрес сервера WINS 192.168.10.2
- **Сервер** SRVR002 **(внешний сетевой адаптер)** — параметры подключения задает провайдер Интернета. Для лабораторного тестирования можно использовать, например, IP-адрес 200.200.200.200 и маску подсети 255.255.255.240. Ни основной шлюз, ни сервер DNS не являются необходимыми в лабораторных условиях.
- **Клиентские компьютеры** -- настроены на получение параметров протокола IP от сервера DHCP.
- **Общий доступ к подключению Интернета и брандмауэр** — выключены.

IP-адрес внутреннего сетевого адаптера компьютера SRVR002 был изначально 192.168.10.3 (один из адресов диапазона, предназначенного для серверов). Поскольку, так или иначе, сервер SRVR002 будет исполнять роль основного шлюза, изменим его адрес на 192.168.10.1 (см. главу 3).

На всех компьютерах, которые будут подключены к Интернету, должен быть указан адрес основного шлюза — 192.168.10.1. Для компьютеров, адресуемых вручную, необходимо вручную же ввести этот адрес, для компьютеров, адресуемых автоматически, — настроить сервер DHCP для выдачи этого адреса:

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль DHCP.
2. Раскройте контейнер сервера SRVR001 и область «Main office»
3. Правой кнопкой мыши щелкните по контейнеру **Параметры области** и из контекстного меню выберите команду **Настроить параметры.** Появится диалоговое окно **Область — параметры.**
4. Отметьте поле **003 Маршрутизатор,** в поле **IP-адрес** введите адрес 192.168.10.1 и затем нажмите кнопку **Добавить**. Нажатием на кнопку **OK** закройте диалоговое окно.
5. В компьютере PC001 запустите командную строку и введите команду **ipconfig /renew**. После успешного обновления IP-адреса введите команду **ipconfig /all** и затем убедитесь в том, что компьютер PC001 также получил адрес основного шлюза. Это действие проделайте со всеми компьютерами, настроенными на автоматическое получение IP-адреса.

Перед дальнейшими действиями также проверьте правильность порядка сетевых адаптеров компьютера SRVR002. Первым по порядку должен быть адаптер внутренней сети.

25.6.2. Настройка трансляции сетевых адресов

Для настройки трансляции сетевых адресов:

1. Зарегистрируйтесь на SRVR002 как администратор и запустите консоль **Маршрутизация и удаленный доступ.**

Примечание.

Если команда Маршрутизация и удаленный доступ недоступна через меню Пуск, запустите консоль MMC и добавьте к ней оснастку Маршрутизация и удаленный доступ.

2. Правой кнопкой мыши щелкните по контейнеру **Состояние сервера** и из контекстного меню выберите команду **Добавить сервер.**
3. В диалоговом окне **Добавить сервер** отметьте поле **Данный компьютер** и затем нажмите кнопку **OK.** В консоли после этого появится значок сервера SRVR002 с красной пометкой. Она говорит о том, что служба **Маршрутизация и удаленный доступ** не настроена и не запущена.
4. Правой кнопкой мыши щелкните по значку сервера SRVR002 и из контекстного меню выберите команду **Настроить и включить маршрутизацию и удаленный доступ**. Запустится Мастер установки сервера маршрутизации и удаленного доступа. Нажмите кнопку **Далее.**

Примечание.

Вам не удастся запустить Мастер настройки, пока вы не отмените общий доступ к подключению к Интернет.

5. В диалоговом окне **Конфигурация** отметьте поле **Преобразование сетевых адресов (NAT)** и затем нажмите кнопку **Далее.**
6. В диалоговом окне **Подключение к Интернету на основе NAT** обозначьте адаптер, который будет подключать сеть к Интернету и отметьте поле **Обеспечить безопасность на данном интерфейсе.** Затем нажмите кнопку **Далее.**
7. В диалоговом окне **Завершение мастера сервера маршрутизации и удаленного доступа** просмотрите предоставленную информацию и затем нажмите кнопку **Готово.**

Теперь служба **Маршрутизация и удаленный доступ** настроена на автоматический запуск. В консоли управления этой службой можно раскрыть контейнер сервера SRVR002 и просмотреть настройки перевода сетевых адресов. Действуйте согласно следующим инструкциям:

1. В консоли **Маршрутизация и удаленный доступ** щелкните по контейнеру **IP маршрутизация,** и в правом подокне отобразите свойства значка **NAT/простой брандмауэр.**
2. На вкладке **Назначение адресов** обратите внимание на то, что поле **Назначить IP-адреса с помощью DHCP-распределителя** не отмечено. Речь идет об уже упомянутой ранее службе DHCP-диспетчер, которая в нашем варианте настройки отключена. Однако здесь все в порядке, поскольку в сети работает обычный сервер DHCP.
3. На вкладке **Разрешение имен в адреса** обратите внимание на то, что поле **Разрешать имя в IP-адрес для клиентов, использующих службу DNS** не отмечено. Речь идет о службе прокси DNS, необходимости в которой при правильно настроенном сервере DNS нет.
4. Нажатием на кнопку **OK** закройте диалоговое окно.
5. Раскройте контейнер **NAT/простой брандмауэр.** В левом подокне консоли появятся как минимум три сетевых интерфейса.
   Правой кнопкой мыши щелкните по значку интерфейса «LAN» и отобразите его свойства. В диалоговом окне обратите внимание на то, что поле **Локальный интерфейс подключения к локальной сети** отмечено. Нажатием на кнопку **Отмена** закройте это окно.
6. Правой кнопкой мыши щелкните по значку интерфейса «Internet» и отобразите его свойства. В диалоговом окне обратите внимание на то, что речь идет о **Публичном интерфейсе подключения к Интернету.** Одновременно здесь должны быть установлены флажки **Включить NAT на данном интерфейсе** и **Включить основной брандмауэр для этого интерфейса** (эта настройка была сконфигурирована в Мастере установки).

Брандмауэр защищает всю сеть (в том числе и публичный интерфейс) от доступа из Интернета. Однако в направлении из внутренней сети в Интернет пользователь никак не ограничен.

Если необходимо ограничить какой-либо трафик в направлении из сети (например, протокол ICMP, то есть отклики на команду PING), действуйте следующим образом:

1. Отобразите свойства интерфейса «Internet» и на вкладке **NAT и простой брандмауэр** нажмите кнопку **Фильтры выхода**. Появится диалоговое окно с таким же названием.
2. Нажмите на кнопку **Создать**. Откроется диалоговое окно **Добавление IP-фильтра**, где вы можете выбрать из списка протокол, обмен по которому собираетесь ограничить, и указать параметры ограничения. Выберите протокол ICMP, поля **Тип ICMP** и **Код ICMP** оставьте пустыми и нажмите кнопку **OK**.
3. Теперь пошлите запрос PING с любого узла вашей сети на любой адрес в Интернете и убедитесь, что ответа не придет.

Настройка фильтрации IP-протокола имеет две особенности. Первая, настройка по умолчанию, её мы уже использовали, говорит о том, что могут проходить любые пакеты, кроме указанных. Вторая же, наоборот, говорит о том, что могут проходить лишь указанные. Фильтрацию протокола IP, таким образом, необходимо хорошо продумать для того, чтобы не пришлось создавать больше правил, чем это реально необходимо.

25.6.3. Доступ извне к ресурсам локальной сети

Настройка доступа, например, к внутреннему веб-серверу никак не отличается от настройки, которую мы привели для общего доступа к Интернету. Для настройки этих подключений в диалоговом окне **Свойства: Интернет** служит вкладка **Службы и порты**, на которой внутренние ресурсы настроены подобно тому, как для функции общего доступа к подключению Интернета. Другая ситуация возникает в случае, когда необходимо предоставить доступ к большему количеству веб-серверов и все на 80 порт.

Хотите вы того или нет, для этой ситуации вам необходимы два публичных IP-адреса. Если пользователь извне обратится к порту 80 по первому адресу, его запрос будет перенаправлен, например, на компьютер PC001. Если кто-то обратится к порту 80 по второму адресу, его запрос будет перенаправлен на компьютер PC002.

Настройка доступа к двум внутренним веб-серверам

Конфигурация доступа к большему количеству внутренних веб-серверов будет складываться из нескольких шагов:

- Получение второго IP-адреса для внешнего интерфейса.

- Определение пула адресов (диапазона публичных IP-адресов, известных в Интернете).
- Переадресация запросов на конкретные серверы.

Присвоение второго IP-адреса

Второй IP-адрес не может быть задан произвольно, его необходимо получить у провайдера подключения к Интернету. Пока предположим, что провайдер кроме адреса 200.200.200.200 выделил нам также адрес 200.200.200.199. Добавьте этот адрес с маской подсети 255.255.255.240 к сетевому подключению по имени «Internet».

Определение пула адресов и доступность внутренних ресурсов

1. Зарегистрируйтесь на SRVR002 и запустите консоль **Маршрутизация и удаленный доступ**.
2. В левом подокне щелкните по контейнеру **Протокол NAT и брандмауэр,** затем в правом подокне отобразите свойства интерфейса «Internet».
3. На вкладке **Пул адресов** нажмите кнопку **Добавить,** появится диалоговое окно **Добавить фонд адресов.**
4. В поле **Начальный адрес** введите адрес 200.200.200.199, в поле **Конечный адрес** -- адрес 200.200.200.200. В поле **Маска** введите значение 255.255.255.240, затем нажмите на кнопку **OK.**
5. Нажмите на кнопку **Применить** и перейдите на вкладку **Службы и порты.**
6. Отметьте службу **веб-сервер HTTP** и в диалоговом окне **Настроить службу** оставьте значения по умолчанию, лишь для поля **Приватный адрес** введите IP-адрес компьютера PC001. Нажмите на кнопку **OK**.
7. Нажмите кнопку **Добавить** и в диалоговом окне **Добавить службу** введите параметры веб-сервера на PC002: переключатель **Публичный адрес** установите в положение **Из пула адресов** и выберите значение 200.200.200.199; в качестве приватного адреса укажите адрес компьютера PC002; в поля внутреннего и внешнего портов введите значение 80.
8. Нажатием на кнопку **OK** закройте все диалоговые окна.

Эти действия можно рассматривать как системное решение. Пользователи всегда ожидают, что веб-сервер работает по порту 80, поэтому номер порта в запросах не указывают. После проведенной настройки они смогут обратиться к обоим нашим веб-серверам.

Менее системным, но более дешевым (не нужно арендовать еще один публичный IP-адрес) было решение, приведенное в п.25.6.1, где запрос

перенаправлялся на тот или другой внутренний веб-сервер в зависимости от указанного внешним пользователем порта.

25.6.4. Трансляция имен Интернета

При подключении к Интернету необходимо обеспечить сопоставление IP-адресов адресам Интернета. Если во внутренней сети настроена служба DNS, ситуация проста и компьютеры можно настроить на передачу невыполненных запросов некоторому серверу DNS в Интернете. Действуйте согласно следующим инструкциям:

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль DNS, подключенную к серверу SRVR001 .
2. Правой кнопкой мыши щелкните по контейнеру SRVR001 и из контекстного меню выберите команду **Свойства**.
3. В диалоговом окне SRVR001 — **свойства** перейдите на вкладку **Сервер для передачи**. Проверьте, что в части **Домен DNS** активен пункт **Все остальные домены DNS,** и в поле **Список IP- адресов серверов для ретрансляции** у выбранного домена введите IP-адрес внешнего сервера DNS (полезно использовать IP-адрес, предоставленный провайдером, этот же адрес настроен на внешнем сетевом адаптере). Затем нажмите кнопку **Добавить**.
4. Нажатием на кнопку **OK** подтвердите настройки и закройте диалоговое окно.

Если в сети нет сервера DNS, можно использовать службу прокси DNS. Для ее работы не обязательно настраивать Общий доступ к Интернету. Настройка службы DNS производится так.

1. Зарегистрируйтесь на SRVR002 как администратор и запустите консоль **Сеть и удаленный доступ**.
2. Раскройте контейнер SRVR002 и затем отобразите диалоговое окно свойств значка **Протокол NAT и брандмауэр.**
3. На вкладке **Трансляция IP адресов** установите флажок **Использовать IP адреса для клиентов использующих службу DNS (Domain Name System).**
4. Нажатием на кнопку **OK** закройте диалоговое окно.

Условием функциональности этой настройки является, конечно же, корректная настройка клиентских компьютеров. Все, кто хочет работать с именами в Интернете, должны иметь в качестве сервера DNS IP-адрес компьютера со службой NAT.

25.6.5. Итого о трансляции сетевых адресов

Этот способ подключения к Интернету не требует изменений адресации протокола IP. Он способен принять любой IP-адрес, который можно использовать в сетях, а не только адрес из подсети 192.168.0.0/24. Этим в то же время устраняется ограничение на количество компьютеров, которые возможно подключить к Интернету этим способом.

Трансляцию сетевых адресов (NAT) можно настроить лишь в системах Windows Server 2003 и Windows 2000 Server. При помощи протокола NAT можно подключаться к внутренней сети через несколько публичных IP-адресов. Более того, возможно фильтровать трафик протокола IP на конкретных внутренних и выделенных IP-адресах.

Службы DHCP-диспетчер и прокси DNS не обязательны. В настройках по умолчанию они отключены.

25.7. Итоги

Если вы хотите подключить свою сеть к Интернету, для этой цели совершенно не обязательно покупать дополнительное программное обеспечение, поскольку требуемые для этого функции предоставлены в системах Windows 2000/XP/2003.

Для небольшой сети без домена вполне достаточно функции Общего доступа к Интернету. Эту функцию можно настроить как в серверных операционных системах, так и в системах для клиентских компьютеров. Эта служба автоматически запускает DHCP-диспетчер и Прокси DNS, которые нельзя ни настроить, ни отключить. Локальному интерфейсу на компьютере, который предоставляет свое подключение к Интернету в общий доступ, автоматически присваивается IP-адрес 192.168.0.1, и служба DHCP-диспетчер присваивает клиентским компьютерам следующие IP-адреса из подсети 192.168.0.0/24.

В области безопасности этого подключения (то есть защиты внутренней сети от доступа из Интернета) системы Windows XP и Windows Server 2003 имеют преимущества, поскольку они содержат встроенную функцию брандмауэра. Хотя она по умолчанию не включена, это вопрос установки одного-единственного флажка. Дальнейших средств обеспечения безопасности подключения этого типа не существует.

В домене или просто большой сети, разделенной на подсети, подключение типа Общий доступ использовать невозможно по причине ограничения адресации протокола IP. Для таких сетей предназначено подключение через трансляцию сетевых адресов (NAT). Этот тип подключения имеет больше возможностей настройки. Он не ограничена лишь подсетью

192.168.0.0/24, и для доступа к средствам внутренней сети из Интернета можно использовать большее количество публичных IP-адресов.

Так же, как при подключении типа Общий доступ, можно защищать всю внутреннюю сеть брандмауэром. Более того, в данном случае можно ограничить конкретный трафик в направлении из сети к Интернету.

Правила ограничения можно определить на основании IP-адресов, но не на основании членства в группах в домене Active Directory. Также нельзя, например, ограничить доступ к конкретным веб-серверам, которые в своём имени содержат запрещенные слова. Для этих целей необходимо установить дополнительное программное обеспечение — например, ISA Server 2000.

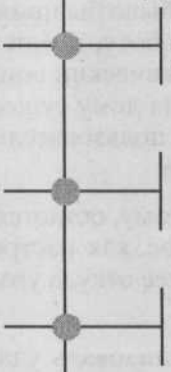
Состояние сети

С этого момента сеть подключена к Интернету. Подключение обеспечивается посредством службы трансляции сетевых адресов (NAT) на сервере SRVR002, на котором для этой цели установлен второй сетевой адаптер. О выделении IP-адресов и других параметров (в том числе и адреса основного шлюза) далее заботится служба DHCP, а о трансляции имен — служба DNS. Запросы на трансляцию внешних имен она отправляет внешнему серверу DNS, адрес которого вы получили у провайдера.

Поскольку сервер SRVR002 является основным шлюзом, его IP-адрес был вручную исправлен на 192.168.10.1.

В Интернет и обратно ходят пакеты любых протоколов, кроме ICMP, запрещенного полностью. Поэтому из внутренней сети нельзя проверить доступность внешних узлов по команде PING. Такая настройка фильтра не слишком полезна, она приведена только как пример возможностей фильтрации протоколов. Можете ее удалить.

Глава 26 Настраиваем удаленный доступ к сети. Если пользователям нужно работать из дома



Очевидно, что большинству пользователей было бы приятно, если бы им не пришлось бы каждый день ходить на работу, и они могли работать дома. Это скорее психологический, чем технический вопрос, потому что средства обеспечения нормальной работы на дому существуют уже давно, вопрос же заключается в том, смогут ли пользователи заставить себя работать столь же успешно, как и на работе.

Решение вопроса, разрешать ли работу на дому, остается за руководителями предприятия. Для нас же важен вопрос, как настроить сеть таким образом, чтобы пользователь мог входить в нее откуда угодно — из своего подразделения, дома или кафе.

Существует несколько возможностей организовать удаленный доступ к сети, и выбор между ними зависит от конкретных требований, в том числе требований безопасности. Например, абсолютно недопустимо, чтобы при подключении пользователя к домену его регистрационные данные передавались в незашифрованном виде; то же обычно относится и к данным.

В этой главе мы рассмотрим возможные решения задачи удаленного доступа, его безопасности, и, как обычно, примеры конкретных ситуаций.

26.1. Не остаться ли нам, администраторам, тоже дома?

Если вы можете себе это позволить, то почему бы и нет?

Администратор типа «прислуга за все», занятый еще и консультированием пользователей, этого позволить себе не может. Даже если на всех рабочих станциях установлена Windows XP Professional — единственная на сегодня

клиентская операционная система, предоставляющая удаленный доступ к рабочему столу, — то далеко не всякий пользователь сможет внятно описать свою проблему; более того, многие просто боятся, когда кто-то берет на себя управление их компьютером, и скорее выключат его, чем разрешат удаленный доступ.

Если же вы управляете своим доменом концептуально, сосредоточившись на его главных функциях и развитии, а повседневные задачи возложили на подчиненных администраторов, то работа из дома может стать для вас неплохой альтернативой. Она станет еще более эффективной, если вы установите в сети программный продукт, который будет активно (в форме SMS-сообщений) обращать ваше внимание на сбои в работе отдельных компьютеров. В этом случае вы не должны целый день проводить у компьютера и можете заниматься другими делами, реагируя на сообщения о проблемах.

Однако оставим теорию. Каждый администратор или пользователь должен сам решить, может ли он выполнять всю свою работу в режиме удаленного доступа и будет ли это выгодно.

26.2. Возможности удаленного доступа

Удаленный доступ к сети состоит из трех основных компонентов: клиента, выполняющего соединение с сетью, сервера, к которому подключается клиент, и среды передачи данных, которая и определяет тип удаленного подключения.

26.2.1. Телефонное подключение

Телефонное подключение к сети используется большинством пользователей, имеющих дома компьютер, и, возможно, они даже не знают об этом. Абсолютное большинство таких пользователей, например, подключаются к Интернету по вечерам, чтобы найти интересную для них информацию или, скажем, проверить почту. Это и есть типичное подключение к сети, в данном случае к сети Интернет. Если это функционирует в случае Интернета, то, само собой, должно работать и в меньших сетях, к которым относится и наша сеть.

Обычно телефонное подключение к сети состоит из следующих компонентов: компьютера-клиента, сервера и двух модемов. Тип модемов зависит от возможностей линии и запросов организации. Можно встретиться с аналоговыми модемами или модемами ISDN, также на серверах можно столкнуться с модемными пулами, которые обеспечивают одновременное подключение нескольких десятков или сотен пользователей, или с моде-

мами ADSL. Однако во всех случаях принцип работы одинаков и можно говорить просто о модеме, безо всякой конкретизации.

Невыгодная сторона этого способа подключения — это его цена. Хотя темп развития компьютерных и технических разработок невероятно высок и цены постоянно падают, в телекоммуникационном бизнесе преобладают гораздо более консервативные способы ведения дел. Особенно в том, что касается цен. Если пользователь собирается подключаться только из своего дома, который обслуживается той же телефонной станцией, что и сервер, то цена будет еще терпима, но для сотрудника, находящегося за границей на деловом совещании, такой способ подключения к сети предприятия явно дороговат.

Несмотря на стоимость, телефонное подключение имеет и ряд выгодных сторон. Его настройка на собственных компьютерах доступна большинству опытных пользователей, а коммуникация «компьютер — сервер» относительно безопасна, то есть к передаваемым данным имеет доступ значительно меньше людей, чем при соединении с Интернетом.

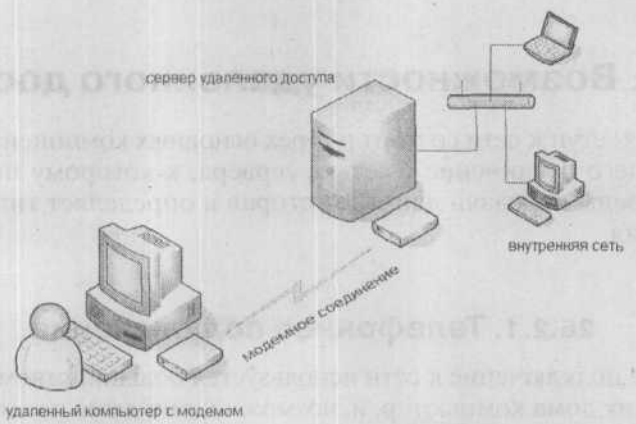


Рис. 26.1. *Для телефонного соединения с локальной сетью требуются модемы на обеих сторонах*

26.2.2. Подключение через виртуальную частную сеть (VPN)

В предыдущей главе мы настроили подключение сети к Интернету, полностью функциональное и не ограниченное по времени. С домашнего или портативного компьютера, имея модем, тоже можно подключаться к Интернету. Нельзя ли соединить эти возможности, то есть использовать

модем на стороне пользователя и постоянное подключение предприятия к Интернету для входа пользователя в сеть предприятия?

Конечно, можно. Если у вас в распоряжении есть модем, то что может быть для вас дешевле и удобнее, чем подключение к сети предприятия через Интернет? Такое подключение носит название виртуальной частной сети (Virtual Private Net).

Технология VPN предоставляет возможность подключения к локальной сети предприятия с помощью ресурсов публичной сети (в том числе Интернета). Она объединяет преимущества подключений удаленного доступа с простотой и гибкостью подключений к Интернету. Чтобы войти в сеть предприятия, достаточно установить соединение по местной линии с любым Интернет-провайдером. Если и домашний компьютер, и локальная сеть используют высокоскоростное подключение к Интернету (например, по технологии DSL), то между ними можно организовать канал обмена данными, пропускная способность которого будет во много раз превышать пропускную способность соединения через обычный модем.

Виртуальные частные сети шифруют пересылаемые данные и проверяют подлинность пользователя, что гарантирует конфиденциальность данных предприятия. Безопасность данных обеспечивается передачей их по протоколам PPTP (Point-to-Point Tunneling Protocol) и L2TP (Layer Two Tunneling Protocol). В процессе работы этих протоколов создаются туннели, обеспечивающие высокую защищенность данных при передаче между компьютерами через Интернет.

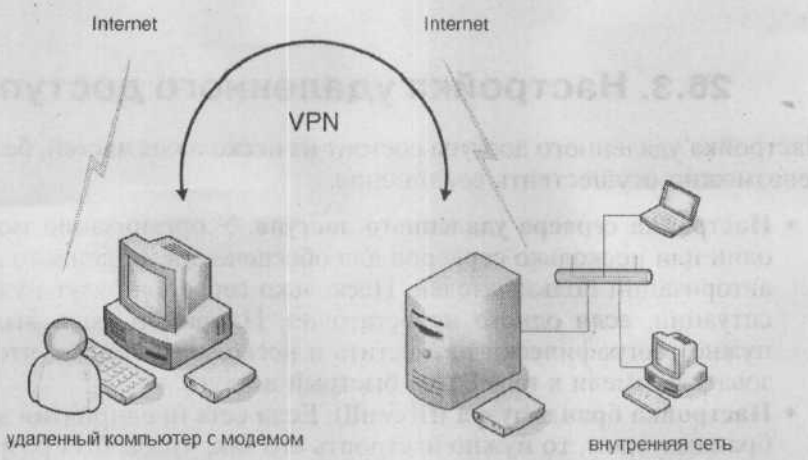


Рис. 26.2. *Принцип виртуальной частной сети (VPN), использующей Интернет*

По сравнению с непосредственным телефонным соединением, подключение через Интернет дешевле, особенно если учитывать не только работу из дома, но и командировочных сотрудников с портативными компьютерами, которым больше не нужно звонить по межгороду, а достаточно подключиться к местному провайдеру.

Еще одним преимуществом VPN перед телефонным соединением является универсальность этого способа. К серверу удаленного доступа сети VPN могут подключаться не только пользователи, входящие в Интернет через обычный модем, но и постоянно подключенные к Интернету по ADSL, по кабелю Ethernet или из локальной сети, подобной той, которую мы настроили в предыдущей главе.

Обычно подключение через Интернет имеет один очень серьезный недостаток — из-за простоты используемых протоколов (HTTP, SMTP и т.д.) стандартные средства связи, используемые в Интернете, не имеют никаких средств защиты доступа. А если вы входите через Интернет в сеть, где размещена важная информация, обеспечение безопасности этих данных — задача номер один. То же самое можно сказать и об аутентификации пользователя при подключении к локальной сети — протоколы аутентификации не всегда обеспечивают достаточную степень безопасности (об этом далее).

Сети VPN дают возможность в продуктах компании Microsoft определить один из двух доступных протоколов для обеспечения безопасности передачи данных, причем у одного из них можно также использовать возможности цифровой подписи передаваемых данных. Более крупные компании даже могут использовать Интернет и технологию VPN для подключения своих филиалов.

26.3. Настройка удаленного доступа

Настройка удаленного доступа состоит из нескольких частей, без которых невозможно осуществить соединение.

- **Настройка сервера удаленного доступа**. У организации может быть один или несколько серверов для обеспечения удаленного доступа и авторизации пользователей. Несколько серверов будут нужны в той ситуации, если одного недостаточно. Например, если эти серверы нужно географически разместить в нескольких точках, чтобы пользователи имели к ним более быстрый доступ.
- **Настройка брандмауэра (firewall)**. Если сеть предприятия защищена брандмауэром, то нужно настроить его так, чтобы был разрешен доступ через нужные порты. В противном случае все попытки доступа компьютеров извне закончатся неудачно.

- **Настройка компьютеров пользователей**. Конфигурация компьютеров всецело находится в распоряжении пользователей. Администратор может упростить их задачу, подготовив файл с расширением INS, который произведет конфигурацию этого подключения. Один из инструментов, помогающих это сделать, — Internet Explorer Administration Kit (IEAK) который можно скачать для различных версий браузера с сайта Microsoft. Этот инструмент, однако, решает не все проблемы, так что администратор должен уметь помочь пользователю настроить подключение.

26.3.1. Телефонное подключение

Поскольку в этом случае на обеих сторонах (на сервере и на компьютерах пользователей) необходимо иметь модем, нужно в первую очередь установить его. Установите модем на сервере SRVR002 и рабочей станции PC001. Затем можете начать саму настройку.

Настройка сервера удаленного доступа

Сервер удаленного доступа предназначен для приема входящих звонков от удаленных компьютеров, которым тем самым предоставляется доступ к ресурсам внутренней сети. Этот сервер является компонентом Windows Server 2003 и устанавливается при установке операционной системы, однако изначально он не настроен и не активизирован. Настройка сервера удаленного доступа проводится через оснастку **Маршрутизация и удаленный доступ** (Routing and Remote Access, RRAS).

1. Зарегистрируйтесь на SRVR002 как администратор и запустите консоль **Маршрутизация и удаленный доступ** из группы **Администрирование**.
2. В окне консоли щелкните правой кнопкой мыши по контейнеру сервера SRVR002 и отобразите его свойства.
3. На вкладке **Общие** флажок **маршрутизатор** будет уже установлен. Поставьте переключатель в положение **локальной сети и вызова по требованию** и установите также флажок **Сервер удаленного доступа**.
4. Отобразится сообщение о необходимости перезапуска службы **Маршрутизация и удаленный доступ**. Ответьте **Да**. В консоли **Маршрутизация и удаленный доступ** появится два новых контейнера — **Порты** и **Удаленные пользователи**. На этом основную настройку на стороне сервера можно считать законченной. Осталось настроить порты для удаленного подключения с помощью модема.
5. Щелкните правой кнопкой мыши по контейнеру **Порты** и отобразите его свойства. Убедитесь, что в списке устройств присутствует модем. В столбце **Число портов** указано максимальное количество

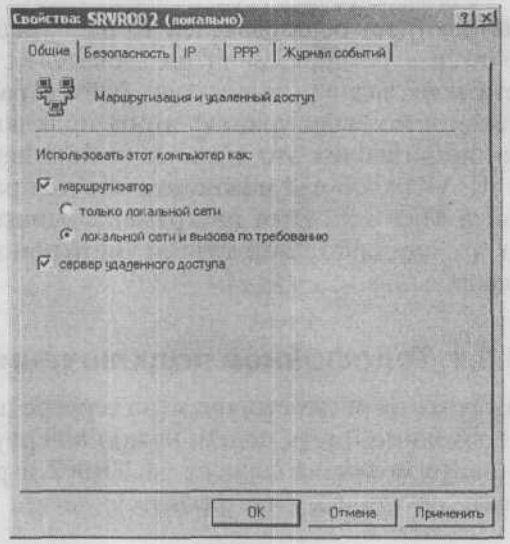


***Рис. 26.3**. Разрешение удаленного доступа*

клиентов, которые могут быть одновременно подключены по этому интерфейсу.

6. Выберите из списка устройств модем и нажмите кнопку **Настроить**.
7. В диалоговом окне настройки установите флажок **Подключение удаленного доступа (только входящие)** и нажмите **OK**.
8. Нажатием на кнопку **OK** закройте диалоговое окно свойств портов.

Настройка компьютера пользователя

Следующий пример приведен только для наглядности. Какие подключения и какого типа следует настроить, зависит от потребностей конкретного пользователя.

1. Зарегистрируйтесь на PC001 как рядовой пользователь. Из главного меню выберите **Панель управления → Сетевые подключения**.
2. В левой части окна **Сетевые подключения** выберите задачу **Создание нового подключения**. Запустится Мастер новых подключений. Нажмите кнопку **Далее**.
3. В диалоговом окне **Тип сетевого подключения** поставьте переключатель в положение **Подключить к сети на рабочем месте** и нажмите **Далее**.
4. В диалоговом окне **Сетевое подключение** поставьте переключатель в положение **Подключение удаленного доступа** и нажмите **Далее**.
5. В диалоговом окне **Имя подключения** введите в поле **Организация** название, под которым оно будет отображаться в списке всех под-

ключений. Оно не обязано совпадать с названием нашего предприятия. Нажмите **Далее**.

6. В диалоговом окне **Номер телефона** задайте номер, который будет набираться при выборе этого подключения и нажмите **Далее**.
7. В диалоговом окне **Доступность подключения** оставьте переключатель в положении **Доступен любому пользователю**, если вы создаете это подключение для всех пользователей данного компьютера; иначе установите его в положение **Только для меня**. Затем нажмите **Далее**.
8. В диалоговом окне **Завершение создания нового подключения** вы можете добавить ярлык этого подключения на рабочий стол. Завершите работу Мастера нажатием кнопки **Готово**.

Окно вновь созданного подключения откроется автоматически. Чтобы проверить это подключение, введите имя пользователя и пароль, а затем нажмите кнопку **Вызов**. Если подключение пройдет успешно, все в порядке. Если нет — проверьте правильность телефонного номера, регистрационных данных пользователя, параметры модема и разрешение на удаленный доступ в домене Active Directory.

Проверка разрешений пользователя в домене Active Directory

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль **Active Directory — пользователи и компьютеры.**
2. Отобразите свойства учетной записи, под которой собираетесь подключаться к сети, и нажмите кнопку **Подключение удаленного доступа**. Доступ можно разрешить, запретить или регулировать при помощи групповых политик.

Если домен работает в смешанном режиме Windows 2000, то в вашем распоряжении будут только первые две возможности. В основном режиме Windows 2000 (native) или Windows 2003 доступны все три возможности. Значение разрешения по умолчанию в смешанном режиме Windows 2000 — **Запрет**, в других режимах — **Управление на основе политики удаленного доступа**. Таким образом, ни в одном из режимов сразу же, без дополнительной настройки, к серверу удаленного доступа подключиться нельзя.

26.3.2. Подключение через виртуальную частную сеть (VPN)

Для подключения посредством виртуальной частной сети вам нужно иметь: действующее соединение с Интернетом на обеих сторонах; настроенный сервер удаленного доступа; брандмауэр на выходном шлюзе

локальной сети; созданное сетевое подключение на клиентском компьютере. Сейчас мы настроим все это в нашей сети.

Настройка сервера

Сервером виртуальной частной сети служит сервер удаленного доступа, который вы настроили в предыдущем параграфе. Чтобы дополнительно настроить его для обслуживания VPN, выполните следующее:

1. Зарегистрируйтесь на SRVR002 как администратор и запустите консоль **Маршрутизация и удаленный доступ**.
2. Отобразите окно свойств контейнера **Порты**. Из списка устройств выберите **Минипорт WAN (PPTP)** и нажмите кнопку **Настроить**.
3. Установите флажок **Подключение удаленного доступа (только входящие)**. В поле **Максимальное число портов** введите значение, равное количеству клиентских компьютеров плюс один — для сервера (то есть, указав 20 портов, можно подключать одновременно 19 компьютеров).
4. Точно так же настройте устройство **Минипорт WAN (L2TP)**.

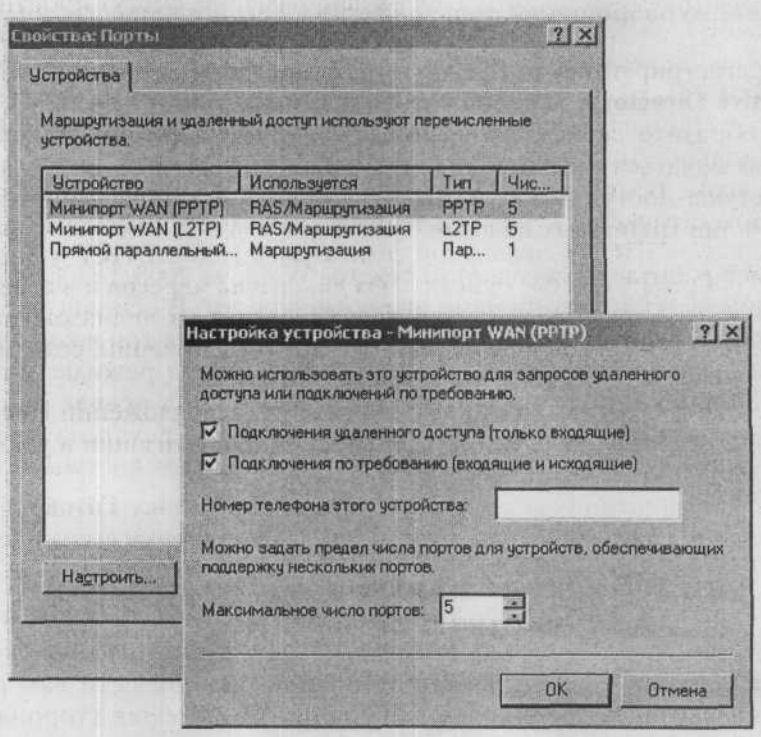


Рис. 26.4. *Настройка порта*

Если служба **Маршрутизация и удаленный доступ** у вас не активирована, поступайте следующим образом:

1. Зарегистрируйтесь на SRVR002 как администратор и запустите консоль **Маршрутизация и удаленный доступ**.
2. Щелкните правой кнопкой мыши по контейнеру SRVR002, отмеченному красным значком. Из контекстного меню выберите команду **Настроить и включить маршрутизацию и удаленный доступ.** Запустится Мастер установки сервера удаленного доступа. Нажмите **Далее**.
3. В следующем окне установите переключатель в положение **Сервер удаленного доступа** и нажмите **Далее**.
4. В окне **Удаленный доступ** установите флажок **VPN** (если вы собираетесь использовать этот сервер также для приема входящих звонков, установите оба флажка). Нажмите **Далее**.
5. В окне **Подключение виртуальной частной сети** отметьте сетевой интерфейс, через который сервер подключен к Интернету (в нашем случае «Internet»). Если вы оставите установленным флажок **Разрешить фильтрацию пакетов,** то все проходящие через этот интерфейс пакеты (входящие и исходящие) будут автоматически фильтроваться так, что в обоих направлениях смогут пройти только пакеты протоколов PPTP и L2TP. Это более безопасный режим, но он приведет к трудностям у тех пользователей, которые подключаются к Интернету, например, через преобразователь сетевых адресов (NAT). Если у вас будут такие пользователи, снимите этот флажок. Нажмите **Далее**.
6. В окне **Назначение IP-адреса** оставьте установленным флажок **Автоматически**, чтобы удаленный компьютер получал IP-адрес от сервера DHCP в локальной сети. Если служба DHCP у вас в сети не работает, можете отметить **Из диапазона адресов** и в следующем окне указать этот диапазон. Первый адрес из диапазона получит виртуальный интерфейс для входящих подключений, созданный на сервере удаленного доступа.
7. В следующем окне оставьте переключатель в положении **Нет, запросы на подключение проверяет служба маршрутизации и удаленного доступа.** Нажмите **Далее.**
8. Для завершения работы Мастера нажмите кнопку **Готово**. Отобразится предупреждение о необходимости установки агента передачи DHCP. Нажмите **Да**.

Отличие этой конфигурации от предыдущей заключается в том, что порты теперь автоматически настроены на прием входящих подключений, количество которых для каждого протокола — 128.

Настройка компьютера пользователя

Работу виртуальной частной сети мы проверим в лабораторных условиях, с рабочей станции PC001. От обычного подключения к локальной сети новое будет отличаться шифрованием передаваемых по нему данных.

1. Зарегистрируйтесь на PC001 как рядовой пользователь. Из главного меню выберите **Панель управления → Сетевые подключения**.
2. В левой части окна **Сетевые подключения** выберите задачу **Создание нового подключения**. Запустится Мастер новых подключений. Нажмите кнопку **Далее**.
3. В диалоговом окне **Тип сетевого подключения** поставьте переключатель в положение **Подключить к сети на рабочем месте** и нажмите **Далее**.
4. В диалоговом окне **Сетевое подключение** поставьте переключатель в положение **Подключение к виртуальной частной сети** и нажмите **Далее**.
5. В диалоговом окне **Имя подключения** введите в поле **Организация** название, под которым оно будет отображаться в списке всех подключений. Оно не обязано совпадать с названием нашего предприятия. Нажмите **Далее**.
6. Если на PC001 настроено телефонное подключение к сети, то в диалоговом окне **Публичная сеть** у вас есть возможность указать, что этот телефонный номер должен быть набран перед подключением к VPN. Если вы не хотите его набирать, установите флажок **Не набирать номер для предварительного подключения**. Нажмите **Далее**.
7. В окне **Выбор сервера VPN** укажите IP-адрес того сервера, к которому вы будете подключаться для входа в сеть VPN (если условия действительно лабораторные, и реального выхода в Интернет с сервера SRVR002 нет, то это будет адрес 200.200.200.200 — см.предыдущую главу). Нажмите **Далее**.
8. В диалоговом окне **Доступность подключения** оставьте переключатель в положении **Доступен любому пользователю**, если вы создаете это подключение для всех пользователей данного компьютера; иначе установите его в положение **Только для меня**. Затем нажмите **Далее**.
9. В диалоговом окне **Завершение работы мастера новых подключений** у вас есть возможность поместить его значок на рабочий стол, установив соответствующий флажок. Закройте диалоговое окно нажатием кнопки **Готово**.

После этого автоматически запустится процесс подключения. Введите имя и пароль пользователя, имеющего разрешение на удаленное подключение, а затем нажмите на кнопку **Подключение**. Если попытка подключиться к виртуальной частной сети окажется неудачной, проверьте настройки сервера, настройку портов протокола PPTP для входящих вызовов, настройку компьютера пользователя и фильтрацию пакетов на интерфейсе с IP-адресом 200.200.200.200.

Если подключение состоялось, вы можете проверить, как оно действует:

1. На PC001 отобразите состояние активного в данный момент сетевого подключения (VPN).
2. Перейдите на вкладку **Сведения** и проверьте несколько важных данных:
   - **Имя устройства**: определяет протокол, по которому осуществляется подключение (PPTP).
   - **Аутентификация** — протокол MS CHAP V2 предоставляет очень сильную защиту регистрационных данных пользователя.
   - **Шифрование** — используется алгоритм шифрования MPPE 128.
   - **IP-адрес сервера и IP-адрес клиента** — адреса, полученные от сервера DHCP.

IP-адрес компьютера-клиента и другие параметры должны отобразиться на локальном компьютере PC001 при вводе команды **ipconfig /all** в режиме командной строки. Если вы хотите проверить, функционирует ли шифрование связи через протокол сети VPN, действуйте следующим образом:

1. Зарегистрируйтесь на PC001 как администратор.
2. В меню **Пуск** нажмите **Выполнить** и в поле **Открыть** введите путь \\192.168.10.38 (IP-адрес сервера VPN мы узнали, пользуясь вышеприведенными инструкциями). Отобразится окно Проводника **Windows** с общими папками на сервере SRVR002.

Если вы видите это окно, значит, шифрованная связь между SRVR002 и PC001 прошла успешно.

Подключение VPN будет активным, пока пользователь не прервет его.

Если вы желаете установить соединение сети VPN с пространством Интернета (до сего момента тестирование проходило в рамках локальной сети), нужно проверить, а возможно, и установить несколько новых свойств.

IP-адреса серверов DNS, WINS и прочие параметры протокола

При настройке подключения через сеть VPN мы установили, что IP-адрес будет назначать компьютерам-клиентам сервер DHCP локальной сети. Речь идет только об IP-адресе, но не о других параметрах IP-протокола. Однако клиентам понадобятся, например, IP-адреса серверов DNS, ведь в случае успешного подключения через сеть VPN они становятся элементами локальной сети, в которой, скорее всего, они будут работать с компьютерами под теми названиями, под которыми они выступают в локальной сети. Сервис DNS, или, возможно,WINS также необходим этим пользователям.

Как это выглядит в нашей сети?

Все важные сведения можно найти на вкладке Протокол IP в окне свойств сервера удаленного доступа SRVR002.

В верхней части вкладки отображено, что IP-адрес клиенты будут получать от сервера DHCP. Это не вполне точно, поскольку на практике выглядит так: сервер DHCP передаст 10 IP-адресов на сервер удаленного доступа, который непосредственно выдаст их клиентам. Если их запас будет исчерпан, то сервер DHCP передаст ему следующую партию. Это установлено таким образом, что назначение IP-адресов не будет задерживаться при каждом подключении к серверу DHCP.

В нижней части вкладки указано, что для поиска IP-адресов серверов DNS и WINS для удаленных пользователей служит адаптер локальной сети LAN. В большинстве случаев эта настройка удовлетворительна, так как у внутренних адаптеров чаще всего бывают стандартные установки, которые одинаковы у всех компьютеров и должны быть такими же у удаленных пользователей.

Однако может случиться так, что у вас в распоряжении нет оборудования, настроенного для удаленных пользователей должным образом. Тогда должна быть осуществлена конфигурация агента передачи DHCP, который обеспечит передачу правильных параметров с серверов DHCP.

Поскольку пользовательские компьютеры связаны с внешним сетевым оборудованием (в Интернете), необходимо, чтобы это оборудование могло передавать запросы внешнему серверу DHCP. Это можно обеспечить следующим образом:

1. Зарегистрируйтесь на SRVR002 как администратор и запустите оснастку **Маршрутизация и удаленный доступ**.
2. Разверните контейнер сервера SRVR002 и правой кнопкой мыши щелкните по значку **Агент передачи DHCP**, выберите команду **Новый интерфейс**.
3. В диалоговом окне **Новый интерфейс для DHCP Relay Agent** выберите интерфейс для связи с Интернетом и нажмите **OK**. В диалоговом окне свойств определите время, после которого агент передачи начнет работу (2 секунды) и нажмите кнопку **OK**. Интерфейс добавится в контейнер **Агент передачи DHCP,** и вы увидите его в левом подокне консоли.
4. Правой кнопкой мыши снова щелкните по значку **Агент передачи DHCP** и из контекстного меню выберите команду **Свойства**. В поле **Адрес сервера** введите IP-адрес сервера DHCP во внутренней сети (в нашем случае 192.168.10.2) и нажмите **Добавить**. Диалоговое окно закройте нажатием кнопки **OK**.

Удаленное подключение компьютеров, не принадлежащих к вашему домену

Подключение к сети VPN (так же, как и телефонное подключение) вы можете проводить с компьютеров, которые не являются членами домена и, соответственно, не имеют в нем собственных учетных данных.

При входе с таких компьютеров кроме имени и пароля необходимо задать также название домена. Нужно отрегулировать соединение и учетные данные и определить, какое название домена пользователи будут употреблять.

Настройка подключения

Настройку самого подключения проведите на основании вышеприведенной инструкции (когда мы настраивали подключение через сеть VPN для компьютера PC001). Затем действуйте следующим образом:

1. Правой кнопкой мыши щелкните по созданному подключению и отобразите его свойства. В диалоговом окне свойств подключения перейдите на вкладку **Параметры**.
2. Установите флажок **Включать домен входа в Windows** и нажмите кнопку **OK**.
3. Если вы потом запустите подключение, отобразится поле для ввода для задания названия домена.

Каково правильное название домена?

Если вы подключаетесь к сети с доменом Active Directory, при подключении вы можете задать имя домена двумя способами — в формате DNS или в формате NetBIOS. NetBIOS-имя нашего домена — study, DNS — study.local. Мы можем ввести еще одно название — доменное имя Study в Интернете (у него не может быть суффикса local, см.главу 7).

Если пользователи привыкнут указывать при регистрации название домена в форме DNS, они потом смогут разрешить вопрос, которое из названий использовать.

Безопасность удаленного доступа

Поскольку при удаленном доступе, использующем сеть VPN, происходит передача очень важной информации через общедоступную сеть, нужно ясно представлять себе уровень безопасности. Первая информация, которой обмениваются компьютеры, -- имена и пароли при входе. Гарантии безопасности предоставляются использованием протокола аутентификации.

Протоколы аутентификации

Назначение протокола аутентификации — передача регистрационных данных и других данных, служащих для подтверждения подлинности пользователя, между компьютером-клиентом и сервером удаленного доступа. Если проверка на подлинность не пройдена, соединение не устанавливается. Какие контрольные протоколы находятся в нашем распоряжении в данной ситуации и как они обеспечивают безопасность?

- PAP (Password Authentication Protocol). Этот протокол передает пароль в форме обычного текста. Из всех протоколов контроля предоставляет наименьшие гарантии безопасности, должен стоять на последнем месте в списке используемых протоколов и использоваться только в том случае, если компьютеры не способны использовать другие протоколы. Его определенно нельзя посоветовать для передачи пароля администраторов домена.
- SPAP (Shiva Password Authentification Protocol). С точки зрения безопасности находится примерно на том же уровне, что и протокол PAP. Его главная цель — дать продуктам Shiva возможность подключения к удаленным серверам.
- CHAP (Challenge Handshake Authentication Protocol). Этот протокол обеспечивает безопасность без передачи пароля. Вместо пароля передается некоторое число, вычисленное на основании пароля и значения, полученного от сервера удаленного доступа.
- MS CHAP (Microsoft Challenge Handshake Authentication Protocol). Дополнение протокола CHAP от компании Microsoft. Обеспечивает безопасную проверку всех пользователей, использующих сервис LAN Manager. Служит, в основном, для контроля подключений клиентов с более старыми системами Windows.
- MS CHAP v2. Вторая версия протокола MS CHAP дает гарантии безопасного подключения клиентам с операционными системами Windows 2000 и более новыми. Также обеспечивает двухсторонний контроль, проверяя тем самым для компьютера-клиента сервер удаленного доступа.
- EAP (Extensible Authentication Protocol). Речь идет об открытой системе, которая дает другим производителям возможность развивать свои собственные протоколы аутентификации. Протокол EAP не проводит сам по себе никакого контроля, но дает возможность определить конкретный способ проверки. Системы Windows Server 2003 включают методы MD5-Challenge, Protected EAP и TLS. Способ TLS, например, используется при контроле доступа при помощи карты Smart Card.

Чтобы использовать конкретный протокол, он должен быть выбран на обоих концах соединения — на сервере удаленного доступа и на компьютере-клиенте. Поскольку можно настроить несколько протоколов, то обычно используются почти все одновременно, от предоставляющих

большую степень безопасности, до предоставляющих наиболее низкие гарантии.

Система Windows Server 2003 также делает возможным доступ удаленных компьютеров без контроля. Поскольку при таком раскладе кто угодно может присоединиться к сети, лучше и не думать об этом варианте.

Настройка аутентификации на стороне сервера

При настройке сервера об аутентификации не упоминалось — ряд протоколов сервер настроил сам. Если вы хотите изменить настройку по умолчанию, действуйте соответственно следующей инструкции:

1. Зарегистрируйтесь на SRVR002 как администратор и запустите оснастку **Маршрутизация и удаленный доступ**.
2. Правой кнопкой мыши нажмите на пункт сервера SRVR002 и отобразите его свойства. В разделе **Безопасность** нажмите на кнопку **Способы контроля**. Отобразится диалоговое окно под тем же названием, в котором стоят галочки напротив используемых протоколов.

То, что вы видите в диалоговом окне, является изначальной настройкой протоколов контроля — MS CHAP, MS CHAP v2 и EAP. Чтобы клиенты могли зарегистрироваться, они должны использовать хотя бы один из приведенных протоколов. Как это выглядит с точки зрения пользователя?

Настройка аутентификации со стороны клиента

В то время как на стороне сервера при конфигурировании предполагается владение знаниями уровня администраторов, для компьютеров-клиентов предполагается определенный уровень знаний пользователей. Настройка какого-либо подключения также обойдется без запросов способа аутентификации — она сводится к вводу пароля. Пользователям это, определенно, говорит больше, чем надпись MS CHAP v2. И тут, определенно, есть возможность провести более прогрессивную настройку посредством отдельных протоколов.

1. Зарегистрируйтесь на PC001.
2. Отобразите свойства настроенного подключения VPN. В разделе **Безопасность** галочка будет стоять в пункте **Обычные установки**.
3. Поставьте галочку в пункте **Дополнительные (выборочные параметры)** и нажмите кнопку **Параметры**. Отобразится диалоговое окно **Дополнительные параметры безопасности**, в котором будет виден исходный набор протоколов аутентификации — MS CHAP и MS CHAP v2.

Безопасность телефонного подключения

После успешной аутентификации пользователя с удаленного компьютера произойдет соединение с сервером и обмен данными. У телефонного подключения есть также другие возможности, как обезопасить это соединение. Повсеместно мы имеем дело с обратными звонками (Call-back).

Функции обратных звонков действуют таким образом, что при подключении пользователя заработает его канал связи и на основании введенных учетных данных будет набран конкретный номер телефона. Расходы берет на себя компания.

Режим обратного звонка может иметь три значения:

- Без обратных звонков. После идентификации пользователя соединение не прерывается, и связь продолжается до тех пор, пока пользователь ее прервет. Расходы, само собой, идут на счет пользователя.
- Полученный от звонящего. В таком случае пользователь, пройдя регистрацию, должен задать телефонный номер, которое затем наберет сервер и установит связь. Расходы идут на счет компании.
- Обратные звонки всегда на номер. После контроля пользователя соединение прерывается, и сервер в тот же момент набирает номер, указанный в этой графе.

Возможность, которую вы выберете, зависит, прежде всего, от уровня безопасности (вспомните о степени риска). Если, например, подключаться будут только ваши пользователи, можно настроить их учетные данные так, что они сами будут задавать номер, который сервер наберет при обратном звонке. Если вы откроете доступ к своей сети внешним организациям (например, торговым партнерам), нужно задуматься над настройками. Как это может выглядеть на практике, показывает следующий случай:

Вы сделаете своему партнеру стандартную доменную группу учетных данных и разрешите ему удаленный доступ через телефонное подключение. У вас хорошие отношения, поэтому вы будете покрывать расходы на соединение, сконфигурируете обратные звонки так, чтобы пользователь всегда мог ввести обратный телефонный номер.

Представитель партнера, которому вы предоставили соответствующую информацию, в том числе имя и пароль для подключения, ознакомит с ней своих коллег, и повесит имя, пароль и телефонный номер на стенд — почему бы и нет, ведь этот доступ будут использовать несколько сотрудников, не только он сам. Но эту информацию случайно может увидеть и какой-нибудь прохожий, не имеющий ничего общего с компанией вашего партнера — возможно, он просто зашел туда в частном порядке. Затем он опробует доступ из дома, использовав собственный номер, на который сервер сам ему перезвонит. И так он сможет за ваш счет проводить целые

ночи в Интернете, и кроме того, пытаться войти в вашу сеть и получить доступ к данным.

Ситуация однако не так сложна, как может показаться на первый взгляд. Если вы хотите добавить гарантий безопасности, выберите третью возможность — обратные звонки всегда на один и тот же номер. Случайный прохожий, таким образом, никак не сможет использовать увиденное имя и пароль, потому что при присоединении и входе из дома сервер прервет соединение и начнет звонить по телефону, прописанному в параметрах подключения. Кроме того, в фирме таким образом могут узнать, что кто-то нелегально использует ваше имя и пароль.

Другая возможность — использование пункта **Проверять ID звонящего**. Эта функция у вас в распоряжении только в основном (native) режиме Windows 2000 или Windows Server 2003 домена. В это поле вводится телефонный номер, с которого пользователь должен звонить, причем это становится частью процесса контроля. Для их использования нужно, чтобы телефонные системы поддерживали эту функцию.

Другие меры безопасности удаленного подключения

Вне зависимости от типа подключения (телефонное, VPN) можно сделать его еще более безопасным. В диалоговом окне свойств учетных данных пользователя в разделе **Телефонное подключение** стандартно есть возможности **Разрешить доступ** и **Запретить доступ**. Однако это не работает в более крупных сетях или сетях с разнообразными условиями подключения. Отдел безопасности инфраструктуры, например, может потребовать, чтобы пользователи отдела продаж имели удаленный доступ только в рабочее время, хотя администраторы этим временем совершенно не ограничиваются. Или он может потребовать, чтобы пользователи, подключенные через модем, были ограничены временем, а пользователи, присоединенные посредством сети VPN через сетевые карты (постоянный доступ к Интернету), не имели ограничений.

Мы имеем целый ряд возможностей, но тех двух настроек, что приведены выше, недостаточно. Нам нужно сделать доступным пункт **Управление доступом через политики удаленного доступа**, а для этого повысить уровень функциональности домена. Если у вас в домене нет контроллера с системой Windows NT 4.0 (которого в нашем случае, конечно, нет), можно не опасаясь осуществить этот шаг:

1. Войдите в компьютер **PC001** и запустите консоль **Active Directory — пользователи и компьютеры**.
2. Правой кнопкой мыши нажмите пункт домена (study.local) и в отобразившемся меню выберите команду **Повысить функциональный уровень домена**. Отобразится диалоговое окно **Повысить функцио-**

нальный уровень домена. В его верхней части отображен текущий уровень, в нижней — высшие уровни.

3. В диалоговом окне выберите пункт Windows 2000 native и нажмите кнопку **OK**.
4. После отображения сообщения о том, что смена повлияет на весь домен, нажмите кнопку **OK**. Отобразится информация, что функциональный уровень повысился. Это необратимое действие. Нажмите кнопку **OK**.

Если вы отобразите свойства учетных данных пользователя, вы сможете в меню **Телефонное подключение** поставить галочку в пункте **Управлять доменом через политики удаленного доступа**. Этим в игру вводятся другие механизмы безопасности, которые называются **Политики удаленного доступа** и которые можно найти в консоли **Маршрутизация и удаленный доступ**.

Свойства удаленного доступа

В изначальной настройке существуют две основных политики удаленного доступа. Каждая из них состоит из трех частей: условий, решения о доступе и профиля.

В условиях определяется все, чему должен удовлетворять удаленный компьютер или пользователь для того, чтобы это для него работало. Можно, например, использовать информацию о членстве пользователя в группах, актуальном времени, типе сервиса, нужного удаленному пользователю, или, например, протоколе, посредством которого пользователь подтверждает свою подлинность. Примером условия может быть следующее: пользователь, являющийся членом группы Domain Admins, подключается от 8 до 16 часов и использует сеть VPN с протоколом PPTP.

Если к пользователю применимо условие или условия (если их несколько, он должен соблюдать все), то должно последовать решение, будет ли ему разрешен доступ или нет. В приведенном примере в случае исполненных условий доступ будет открыт.

Если доступ был разрешен, то следует очередь третьей части политики, которой является профиль. Его свойства вы можете отобразить нажатием на кнопку **Настроить профиль** в свойствах политики удаленного доступа. Профиль может включать и другую информацию, позволяющую еще больше обезопасить подключение (например, уровень шифровки или контрольный протокол). В менее крупных сетях в профилях используются только ограничения, например, как долго клиент может быть подключен.

После первого знакомства с политиками удаленного доступа вы, может быть, несколько разочарованы. Да, нужно сказать, тут существует много

возможностей конфигурирования, которые могут обезопасить или запретить соединение, и кроме того нужно хорошо осмыслить порядок, в котором проходят отдельные части операции аутентификации и установки соединения.

Рассмотрим случай: как администраторы мы хотим создать следующий порядок:

- Все пользователи могут подключаться посредством сети VPN когда угодно.
- Кроме того, телефонное подключение может использовать только отдел продаж и только в рабочее время (8-16 часов).

Ход настройки будет следующим:

- Настройка всех гучетных записей пользователей для телефонного присоединения на основе политик.
- Конфигурация политик удаленного доступа.
- Контроль настройки.

Настройка учетных данных пользователей

1. Зарегистрируйтесь на SRVR001 как администратор и запустите консоль **Active Directory — Пользователи и компьютеры**.
2. У всех пользователей активируйте в разделе **Телефонное подключение** пункт **Управление доступом посредством параметров удаленного доступа**.

Настройка параметров удаленного доступа

Для настройки параметров удаленного доступа:

1. Зарегистрируйтесь на SRVR002 как администратор и запустите консоль **Маршрутизация и удаленный доступ**.
2. Разверните значок сервера SRVR002 и правой кнопкой мыши нажмите на пункт **Политики удаленного доступа**. В отобразившемся меню выберите команду **Новые политики удаленного доступа**. Запустится Мастер создания новых политик удаленного доступа. Продолжите нажатием кнопки **Далее**.
3. В диалоговом окне **Способ конфигурации параметров** наберите в поле **Названиеназвание Отдел продаж — телефонный доступ**.
4. В диалоговом окне **Способ доступа** поставьте галочку в пункте **Набор номера** и нажмите **Далее**.
5. В диалоговом окне **Доступ пользователя или групп** оставьте галочку в графе **Группы** и нажмите кнопку **Добавить**. В списке доменных групп добавьте группы **«G Shop Regular» и «G Shop Power»** и нажмите **OK**. Продолжите нажатием на кнопку **Далее**.

6. В диалоговом окне **способов аутентификации** оставьте галочку в пункте MS CHAP v2 и нажмите кнопку **Далее**.
7. В диалоговом окне **Уровень шифровки параметров** оставьте галочки в тех графах шифровки, которые нужны пользовательским компьютерам. Если у вас клиентские компьютеры с системами Windows 2000 и более новыми, вы можете оставить только 128-битную шифровку. Продолжите нажатием на кнопку **Далее**.
8. В последнем диалоговом окне просмотрите введенную информацию и нажмите **Готово.**

Примечание.

Возможно, вы заметили, что здесь мы предоставили допуск глобальным группам. Это обстоятельство не очень хорошо вписывается в стратегию разрешения доступа, которой мы руководствуемся. Однако ничего не поделать, ограничение системы таково, что мы не можем здесь использовать доменные группы.

Второй параметр мы настроим таким способом:

1. Правой кнопкой мыши нажмите на пункт **Политики удаленного доступа**. В отобразившемся меню затем нажмите на команду **Новые политики удаленного доступа**. Запустится Мастер создания параметра удаленного доступа. Продолжите нажатием кнопки **Далее**.
2. В следующем диалоговом окне введите в графу **Название** название **Все — доступ через VPN**. Затем нажмите **Далее.**
3. В диалоговом окне **Способ доступа** поставьте галочку в пункте **Через сеть VPN** и нажмите **Далее**.
4. В диалоговом окне **Доступ пользователя или группы** поставьте галочку в графе **Пользователи** и нажмите **Далее**.
5. В диалоговом окне **Способы контроля** оставьте галочку в пункте MS CHAP v2 и нажмите на кнопку **Далее**.
6. В диалоговом окне **Уровень шифровки параметра** оставьте галочки во всех пунктах. Нажмите **Далее**.
7. В последнем диалоговом окне просмотрите введенную информацию и нажмите **Готово**.

В консоли **Маршрутизация и удаленный доступ** должно быть четыре значка политик удаленного доступа — два изначально и два добавились после конфигурации. Политики расположены в определенном порядке, который очень важен. На первом месте должна быть политика **Все** — подключение VPN, а на втором — политика **Отдел продаж — удаленный доступ**. Порядок предустановленных политик не столь важен — ведь обе они запрещают пользователям доступ.

Проверка

Тут не имеет смысла подробно описывать конфигурацию отдельных подключений и, следовательно, (не)подключений конкретных пользователей. Много более интересным будет описание пути, который должны пройти входящие пользователи. Самым важным представляется то, что все пользователи имеют управляемое политиками удаленное подключение. Ход удаленного присоединения любого пользователя выглядит следующим образом:

1. Пользователь подключается и проходит контроль через протокол MS CHAP v2.
2. Система проводит контроль свойств учетной записи пользователя и выясняет, что удаленный доступ управляем политиками удаленного доступа.
3. Для первой политики удаленного доступа (Все — доступ VPN) проводится сравнение с его настройками в действительности — поскольку речь идет о подключении VPN, условия выполнены и принимается решение о доступе. Разрешение доступа настроено, пользователь может двигаться дальше.
4. Система отконфигурирует профиль этой политики. Он может включать только 128-битную шифровку (если вы задали это во время настройки). Если клиент выполняет это условие, то подключение произойдет.

Ход удаленного подключения пользователя отдела продаж при помощи модема будет следующим:

1. Пользователь подключается и проходит контроль по протоколу MS CHAP v2.
2. Система в свойствах пользователя обнаружит, что удаленный доступ управляется политиками удаленного доступа.
3. Подключение не соблюдает условий первой политики — речь не идет о подключении через сеть VPN. Перейдем к следующей политике.
4. Условия второй группы соблюдены — речь идет о подключении через модем (асинхронный или ISDN) и пользователь является членом одной из групп отдела продаж.
5. Политика разрешает доступ, так что остается только проанализировать его. Пользователя может ограничить только недостаточный уровень шифрования клиентской операционной системы. В противном случае пользователь подключится.

Если пользователь, использующий для подключения модем, не является членом какой-либо группы, то в действие вступают следующие политики.Поскольку он удовлетворяет условиям обеих (подключение к серверу Microsoft Routing and Remote Access и присоединение к другим серверам для доступа), него принимается решение о доступе, и это решение — запретить.

Для чего существуют настройки по умолчанию?

На практике может случиться так, что вы вообще не будете использовать политики, потому что домен будет в режиме Windows 2000 mixed или у вас просто не будет необходимости настраивать разрешение на удаленный доступ. Вам просто будет достаточно настройки, есть доступ или нет. В этой связи уместен вопрос, почему существуют изначальные политики.

Их наличие обусловлено самой системой удаленного доступа в системах Windows 2000 Server и Windows Server 2003.

Внимание! Даже если ни для одного пользователя доступ не регулируетсяс помощью политик удаленного доступа, одна из политик вам точно понадобится (условиям которой удовлетворяют все возможные все пользователи). Без нее не подключился бы не один пользователь, хоть доступ и разрешен.

Для большей наглядности на рисунке 26.5 изображен весь ход удаленного подключения.

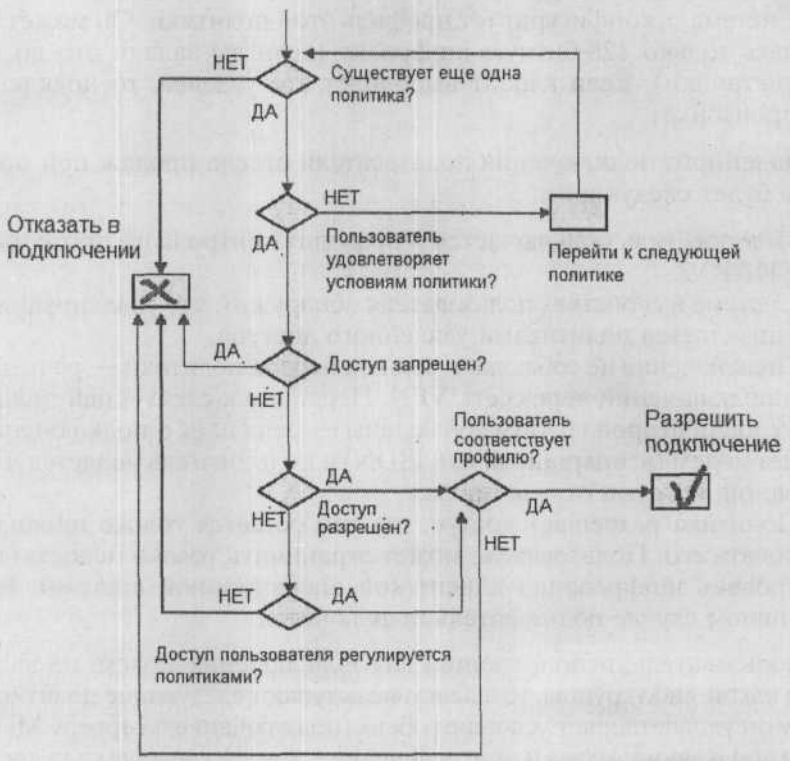


Рис. 26.5. *Наглядное изображение получения разрешения удаленного доступа*

До принятия настройка доступа к удаленному подключению требует еще многих установок. Если у вас несколько различных запросов к доступу через телефонное подключение или VPN, нужно подробно все распланировать, определить несколько конкретных случаев и просмотреть все заданные параметры. Только так вы проверите, что ни о чем не забыли и что пользователи, которые в данное время не имеют права доступа, не могут войти в систему.

Размещение политик удаленного доступа

Политики удаленного доступа всегда размещены в локальном компьютере. Если вам нужно настроить другой сервер удаленного доступа, следует настроить все параметры заново в новом сервере. Если окружение еще более сложно (несколько серверов удаленного доступа), решением может быть настройка сервера RADIUS, в интерпретации компании Microsoft именуемого IAS (Internet Authentication Server).

26.4. Итоги

Пользователи (в том числе администраторы) не обязаны постоянно сидеть на работе перед компьютером, но могут работать и на расстоянии. Однако для этого им нужно настроить доступ к сети.

Цель администраторов — настроить удаленный доступ так, чтобы он был удобен для пользователей и имел гарантии безопасности. Это касается как информации, необходимой для контроля пользователей, так и данных, которыми сеть обменивается с данным компьютером.

Одна из возможностей удаленного доступа — телефонное подключение через модем. Причем модем должен иметься у обеих сторон, в случае подключения нескольких пользователей нужно использовать модемное поле на стороне сервера. Выгодная сторона телефонного подключения — относительно высокие гарантии безопасности, невыгодная — цена. Еще одна возможность удаленного подключения — использование виртуальной частной сети.

Для этого в первую очередь нужно подключиться к Интернету, так как виртуальная частная сеть использует для соединения компьютеров именно его. Поскольку Интернет — не самое безопасное пространство для передачи важных данных, виртуальная приватная сеть обеспечивает достаточный уровень безопасности их шифровкой. Она использует для этого или собственное шифрование (PPTP), или шифрование по протоколу IPSec (это в случае соединения через протокол L2TP).

Кроме настройки сервера удаленного доступа, с точки зрения администратора, нужно настроить свойства учетных записей пользователей. В домене Active Directory в режиме Windows 2000 mixed у вас есть две возможности — разрешить или запретить удаленное подключение. В режиме Windows 2000 native или Windows Server 2003 вы имеете к тому же возможность управлять подключением при помощи политик удаленного доступа. Как раз это предоставляет возможность разделить различные случаи доступа, например, на основании членства в группах, технологии доступа или времени дня.

Политики удаленного доступа очень важны, несмотря на функциональный уровень домена — если ни одной политики не существует, то удаленный доступ не будет разрешен ни одному пользователю, несмотря на то, что домен стоит в режиме Windows 2000 mixed и пользователю в нем может быть разрешен удаленный доступ.

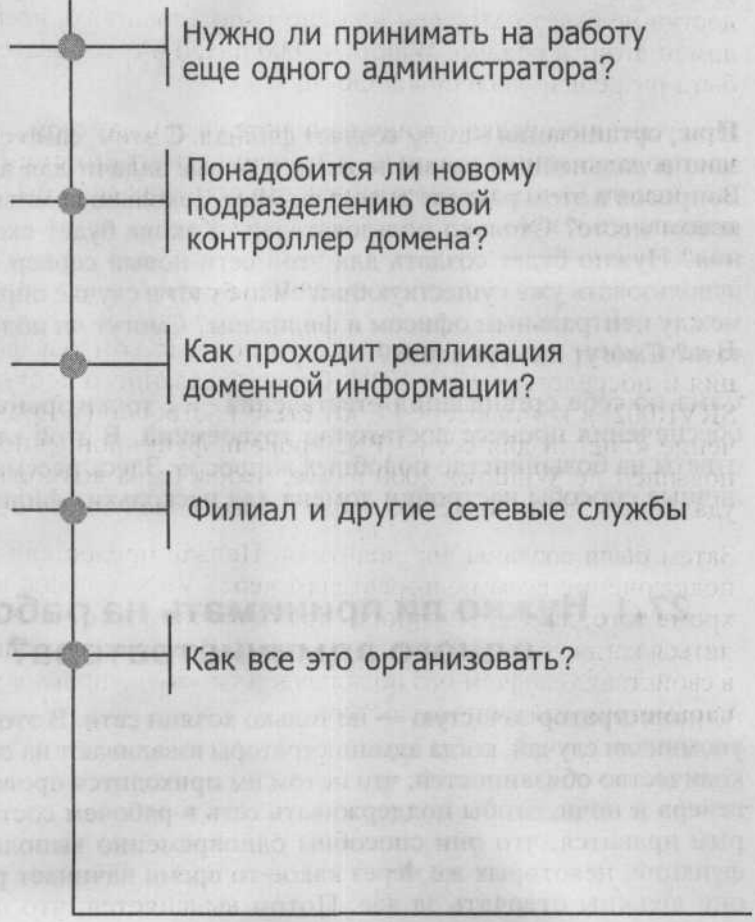
При успешном подключении компьютер в стандартном случае становится частью сети и пользователь, в зависимости от его степени доступа, может использовать те же возможности сети, как если бы он был локально подключен к ней.

Состояние сети

В сети настроен удаленный доступ посредством телефонного соединения и посредством сети VPN. Сервер удаленного доступа -- компьютер SRVR002, в компьютере PC001 было настроено (и проверено) подключение клиента для сети VPN. Уровень функциональности домена был повышен до Windows 2000 native, чтобы была возможность управлять удаленным доступом с помощью политик удаленного доступа.

Затем были созданы две политики. Первая предоставляет возможность подключения всем пользователям через VPN в любое время, вторая — кроме того, дает возможность пользователям из отдела продаж подключиться когда угодно с помощью модема. Все пользователи в домене имеют в свойствах телефонного подключения доступ, управляемый политиками параметрам удаленного доступа.

Глава 27 Предприятие открывает филиал



Итак, организация Study создает филиал. С этим, само собой, будет связано и дальнейшее развитие сети, и новые задачи для администратора. Вопросов в этом разделе довольно много: сколько компьютеров будет на новом месте? Сколько пользователей? Какова будет скорость соединения? Нужно будет создать для этой сети новый сервер или достаточно использовать уже существующий? Что будет в случае обрыва соединения между центральным офисом и филиалом? Смогут ли пользователи работать? Смогут ли они войти?

Сама по себе организация ответвления — с точки зрения технического обеспечения процесс достаточно трудоемкий. В этой главе вы найдете ответы на большинство подобных вопросов. Здесь рассматриваются различные способы настройки домена для нескольких филиалов.

27.1. Нужно ли принимать на работу еще одного администратора?

Администратор зачастую — не только хозяин сети. В этой книге мы уже упоминали случай, когда администраторы взваливают на свои плечи такое количество обязанностей, что потом им приходится проводить на работе вечера и ночи, чтобы поддерживать сеть в рабочем состоянии. Некоторым нравится, что они способны одновременно выполнять несколько функций, некоторых же через какое-то время начинает раздражать, что они должны отвечать за все. Потом выясняется, что они выполняют множество всякой работы (от установки оборудования и обучения пользователей до управления доменом), но ни одна из них не выполняется на сто процентов.

Взвалить на такого администратора работу по планированию структуры сети и управлению подсетью нового подразделения — довольно безрассудная авантюра, ведь у него недостаточно времени даже на обеспечение работоспособности ближайшего сетевого окружения.

Если в компании работает администратор, в ведении которого находится только управление доменом и который не занимается разрешением конкретных трудностей пользователей (ими занимается, например, служба технической поддержки), то весьма правдоподобно, что он сможет спланировать и организовать новое подразделение, найдя для этого достаточно времени. Как будет осуществляться управление новым окружением, когда филиал начнет работу?

27.1.1. Служба поддержки пользователей

Сотрудники этой службы занимаются не непосредственно управлением сетью, а обучением и консультированием пользователей. Их количество обычно прямо пропорционально числу пользователей сети предприятия, и начальнику отдела IT легко решить, следует ли расширять службу поддержки в связи с появлением нового подразделения.

27.1.2. Администраторы сети

Если воспринимать администратора сети как человека, ведающего настройкой и управлением доменом, например, сетевыми службами, то появление нового подразделения определенно не может являться поводом для автоматического приема на работу еще одного сотрудника. Указать примерное количество пользователей, приходящихся на одного администратора, невозможно, поскольку объем работы зависит от конкретных условий предприятия. Можно столкнуться с ситуацией, где на сорок пользователей приходится 5 администраторов, и к тому же иногда приходится пользоваться услугами консультантов извне, однако в то же время можно привести примеры, когда один администратор управляется с несколькими сотнями пользователей и все функционирует без особых трудностей. Причиной такого различия является конфигурация и использование возможностей Active Directory и других сервисов.

Например, тот, кто не использует в достаточной мере групповые политики, делегирование управления или автоматизацию рутинных действий по созданию учетных записей и объединению их в группы, обязательно столкнется со сложностями при расширении предприятия. И наоборот, того, кто как следует подготовился заранее, использует все предоставленные возможности и тщательно документирует сеть, расширение сети не может застать врасплох. В предыдущих главах показано обилие возможностей

домена Active Directory, и если они должным образом документированы и настроены, то вы окажетесь в «лучшей» группе администраторов, которые вовремя уходят с работы, спокойно спят и не видят кошмарных снов о грядущем расширении сети. Они, кстати, избавлены и от другого кошмара — найма дополнительного администратора, который впоследствии может вытеснить их с работы.

27.2. Понадобится ли новому подразделению свой контроллер домена?

После «человеческой» стороны проблемы давайте обсудим техническую сторону. Контроллер домена обслуживает домен Active Directory, авторизует компьютеры и пользователей, применяет к ним объекты групповой политики. Это значит, что с контроллером домена каждый компьютер поддерживает связь при включении, регистрации пользователя и далее, регулярно через определенные временные интервалы.

Если контроллер домена и рабочая станция пользователя соединены слишком медленной линией, в сети могут возникнуть определенные неудобства. Пользователи будут жаловаться на слишком медленный процесс регистрации, на медлительность других сетевых служб, а администраторы через какое-то время могут обнаружить, что некоторые объекты групповой политики не работают так, как задумано.

О скорости соединения не стоит судить лишь на основании номинальной пропускной способности канала связи между филиалом и центральным офисом. Соединение может иметь скорость, скажем, 1 Мбит/с и все-таки быть очень медленным, поскольку затруднено, например, работой пользователей с Интернетом. И наоборот, соединение со скоростью 128 Кбит/с может быть быстрее в некоторых случаях. Не забудьте о применении групповых политик: скорость, при которой половина из них применяться не будет, по умолчанию равна 500 Кбит/с.

Как правило, сеть организуется таким образом, что для компьютеров, подключенных по медленной линии, выделяется собственный контроллер домена. Медленным соединением в Америке считается соединение со скоростью меньше 1.5 Мбит/с, а в наших условиях таким можно считать любую линию, скорость которой меньше скорости локальной сети (составляющей в большинстве случаев 10 Мбит/с).

Если у вас есть подсеть, в которой не более 5 пользователей, или вы собираетесь ее завести, нужно тщательно взвесить, стоит ли устанавливать другой компьютер — контроллер домена. Если же в этом подразделении более 5 пользователей, то вам определенно можно посоветовать устано-

вить его. К тому же этот компьютер также станет файловым сервером, сервером DNS, хранилищем перенаправленных папок «Мои документы» и так далее.

Вам, как администратору домена, это не принесет особых хлопот после инсталляции всего необходимого программного обеспечения, поскольку процессы контроля и другие процессы, связанные с управлением доменом, будут достаточно быстры и пользователи останутся довольны.

27.3. Как проходит репликация доменной информации?

С момента, когда в домене появляется еще один контроллер, клиентские компьютеры смогут выбирать, который из них будет отвечать на их запросы. Это значит, что в новом контроллере должна быть заложена та же информация, что и в старом, чтобы все корректно работало. Этой цели служит. репликация доменной базы данных Active Directory.

Новые объекты (пользователи, группы, компьютеры и т.д.) можно создавать на любом контроллере домена. В консоли **Active Directory — пользователи и компьютеры** этот объект появляется с полным доменным именем. Новый объект автоматически появляется и на остальных контроллерах домена, правда, не сразу. Когда это случится, зависит от сетевой топологии и физического представления сети в домене Active Directory.

27.3.1. Сайт

Для того чтобы полностью осознать приведенную далее информацию о репликации данных между контроллерами домена, нужно ознакомиться с понятием, которое до сих пор в книге не рассматривалось. Это сайт — объект, представляющий физическую организацию сети в домене Active Directory.

Сайт определяется как группа компьютеров (точнее, IP-подсетей), связанных высокоскоростной линией. Под высокой обычно понимают скорость, характерную для локальных сетей (10 Мбит/с и выше). То есть, если у вас в центральном офисе все компьютеры объединены в сеть со скоростью 100 Мбит/с, то с точки зрения домена Active Directory это один сайт. Другое подразделение, подключенное к головному офису линией 128 Кбит/с, будет другим сайтом. Понятие сайта введено для контроля сетевого трафика, относящегося к синхронизации каталога, и обеспечения доступа пользователей к локальным ресурсам для снижения загрузки сети.

Сайт делает сайтом наличие своего контроллера домена, обеспечивающего все возможности, характеризующие сайт с точки зрения активного каталога, а с точки зрения пользователей гарантирующего быструю и беспроблемную работу сети.

От размещения контроллеров домена по сайтам зависит способ репликации доменной базы. Это весьма логично — если подразделение соединено с головным офисом медленной линией (например, 64 Кбит/с), которая весь день занята передачей данных приложений, то вы не захотите загружать ее еще и репликацией доменных данных, которые не имеют особого значения для подразделения. Информация о новой группе учетных записей пользователей, определенно, не настолько важна, чтобы ее необходимо было копировать в ближайшие минуты. И наоборот, контроллеры домена, расположенные в одном сайте, должны быстро обмениваться доменной информацией. Что было бы, если бы вы создали для пользователя новую учетную запись, попросили бы его зарегистрироваться и ничего не получилось бы? В пределах сайта невозможно сказать заранее, какой из контроллеров домена будет выполнять ту или иную функцию, поэтому максимально быстрая репликация важной информации очень важна.

27.3.2. Репликация в пределах сайта

Если в одном сайте находятся несколько контроллеров домена под управлением Windows Server 2003 (положим, A, B, C и D), репликация будет проходить следующим образом:

- Вы создаете новую учетную запись пользователя на сервере A.
- Сервер A ждет 15 секунд, а затем предупреждает первого партнера по репликации. Затем он посылает ему сообщение, что его доменная база данных изменилась. Сообщение следующему партнеру будет отослано через 3 секунды и так далее. Паузы в 3 секунды предназначены для предотвращения перегрузки сети, чтобы контроллеры не пытались скачать обновленную базу одновременно.
- Серверы B, C и D (если они партнеры по репликации сервера A), приняв сообщение об обновлении данных домена, попросят у сервера A дать им возможность скачать информацию об этих изменениях. Сервер A примет запрос и даст возможность скачать ее.

Таким образом, новая учетная запись окажется в распоряжении первого партнера по репликации примерно через 15 секунд. Через какое время она будет на всех контроллерах домена, зависит от топологии репликации.

Топология репликации

Топология репликации автоматически создается компонентом под названием KCC (Knowledge Consistence Checker). Он запускается каждые 15 минут, обходит все контроллеры домена каждого сайта и создает между ними объекты-подключения таким образом, чтобы путь между любыми двумя серверами не был бы длиннее 3 звеньев. Переводя это на язык чисел, любое изменение в домене отобразится на всех контроллерах максимум через 45 секунд.

Примечание.

Контроллеры домена с системой Windows 2000 проводят в рамках сети репликацию доменной базы раз в 5 минут. Этот интервал сильно сокращен в Windows Server 2003.

Интервал 15 секунд, касающийся репликации, невозможно изменить. Нужно смириться с этим и воспринимать как данность. Кроме обычного вида репликации, в домене существует также безотлагательная репликация, которая проводится моментально. Пример такой репликации — закрытие учетной записи пользователя.

Возможности топологии репликации в рамках более крупной организации показаны на рисунке 27.1.

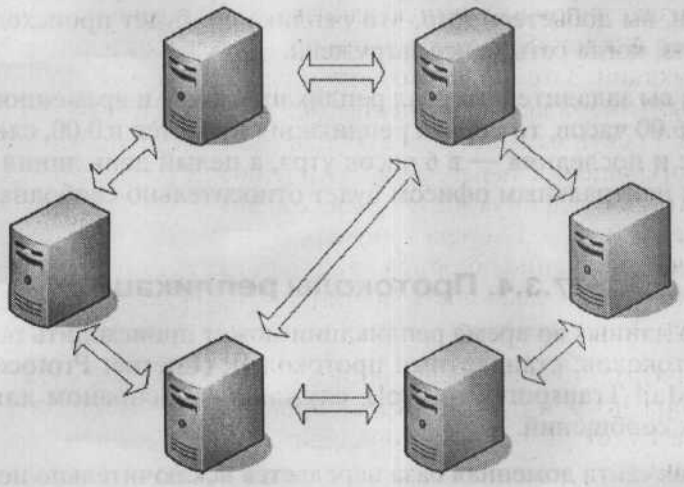


Рис. 27.1. *Между любыми двумя контроллерами домена нет пути длиннее, чем 3 звена*

27.3.3. Репликация между сайтами

Одна из характеристик сайта активного каталога — возможность определять время, когда должна проходить репликация доменной информации. Хотя в пределах сайта интервал составляет 15 секунд и изменению не подлежит, параметры репликации между сайтами вы, как администраторы, можете определять сами. В общем, это понятно — в пределах сайта контроллеры домена всегда связаны быстрым соединением, так что предполагается, что быстрая репликация никак не помешает работе сети. Однако между сайтами это не совсем так. Если организация будет иметь два отделения, в Санкт-Петербурге и в Ярославле, то создание новой учетной записи пользователя в Петербурге не обязано отображаться в ярославском отделении через 15 секунд. Даже через час или три это не обязательно. Некоторые пользователи в Ярославле с удовольствием вообще не загружали бы сеть репликацией, но домен Active Directory просто обязан реплицировать доменную базу каждый раз по прошествии определенного времени. Она необходима, потому что копируются не только учетные записи, безразличные для другого сайта, но и, например, зоны DNS, которыми пренебречь нельзя.

Выбор периода репликации между сетями зависит от администратора. Репликацией заведуют два параметра:

- **Интервал репликации**. Он определяет, как часто будет проходить репликация. Например, 1 час, 3 часа и т.п. Наименьший возможный интервал — 15 минут.
- **Расписание репликации**. Вы можете ограничить репликацию только указанным временем: например, задав временную границу 0.00-6.00 часов, вы добьетесь того, что репликация будет происходить только ночью, когда сеть менее загружена.

Так, если вы зададите интервал репликации 1 час и временное ограничение 0.00-6.00 часов, то первая репликация начнется в 0.00, следующая — через час и последняя — в 6 часов утра, а целый день линия между филиалом и центральным офисом будет относительно свободна.

27.3.4. Протоколы репликации

Передача данных во время репликации может происходить по одному из двух протоколов: стандартный протокол IP (Internet Protocol) и SMTP (Simple Mail Transport Protocol), служащий в основном для передачи почтовых сообщений.

В пределах сайта доменная база передается исключительно по протоколу IP. Такова системная конфигурация, которую администраторы не могут изменить.

Протокол репликации между сайтами можно выбирать. Если речь идет о репликации в рамках одного домена, то возможности опять ограничиваются протоколом IP. Если же репликация осуществляется между доменами (это случай не нашей организации, но скорее более крупных организаций с несколькими доменами, организованными в лес Active Directory), то есть выбор между протоколами IP и SMTP.

Передаваемые доменные данные следует обезопасить, поскольку канал для их передачи обычно предоставляет третья сторона. Если вы настроите передачу по протоколу IP, то они будут шифроваться и сжиматься автоматически. Если вы будете использовать протокол SMTP, то данные тоже будут шифроваться. Для этого у компьютера должны быть необходимые ключи, полученные от сертификационного сервиса сети, (если он настроен), или которые он создаст сам. Следствием будет всегда шифрованная связь по протоколу SMTP.

27.3.5. Другие характеристики сайта

Как уже сказано, основным назначением сайта является управление синхронизацией активного каталога. Если все будет нормально работать, можно предположить, что медленная линия между сайтами будет загружена гораздо меньше, чем если бы вы объединили подразделения в один сайт.

Представьте, например, что центральный офис организации находится в Петербурге, а филиал — в Ярославле. В обоих подразделениях есть контроллеры домена. Администратор настроил репликацию по протоколу IP каждый час круглосуточно. Вы считаете, что обмен данными между контроллерами не затрудняет работу пользователей, но они почему-то жалуются на слишком медленный процесс регистрации в сети.

Пусть это пользователь за компьютером PC111. Зарегистрируйтесь на этом компьютере. После успешной (хотя и долгой) регистрации введите на этом компьютере команду SET. Она выведет значения всех системных переменных. Переменная LOGONSERVER указывает на то, который из контроллеров домена обработал запрос на регистрацию:

```
C:\Documents and Settings\ITManager1>set
...
COMPUTERNAME=PC111
LOGONSERVER=\\SRVR001
...
```

Примечание.

Чтобы не разыскивать одну переменную среди всех системных, вместо команды **set** введите команду **echo %logonserver%**.

Почему же пользователю пришлось так долго ждать? Оказывается, его запрос на регистрацию обработал контроллер домена, расположенный в другом сайте, то есть весь процесс происходил по медленной линии. Для регулирования этого процесса в активном каталоге существует контейнер **Subnets (Подсети)**. Именно здесь определяется привязка компьютера к соответствующему контроллеру домена.

Компьютеры в филиале и центральном офисе отличаются своими IP-адресами, образующими разные подсети. По подсети (адресам и маске) можно однозначно привязать компьютеры к сайтам. Тогда запрос на регистрацию будут обрабатывать те из контроллеров домена и серверов DNS, которые находится в том же сайте, и только при невозможности их ответа запрос будет передан на другой сайт.

27.4. Филиал и другие сетевые службы

В нашей сети мы используем четыре службы — DHCP, DNS, WINS и службу сертификации. Как проходит взаимодействие с ними в случае нескольких филиалов?

27.4.1. Служба DNS

Служба DNS необходима для нормальной работы домена Active Directory. Именно она, преобразуя названия компьютеров в IP-адреса, позволяет найти контроллеры домена и другие серверы, важные для работы сети. До сих пор сервер DNS был установлен только на сервере SRVR001, и зона study.local была настроена как интегрированная в Active Directory (см. рис. 27.2).

Значение параметра **Репликация** «Все контроллеры домена в домене Active Directory» означает, что, если вы инсталлируете еще один контроллер домена, то он автоматически будет содержать зону study.local.

Система Windows Server 2003, в отличие от Windows 2000 Server имеет несколько вариантов размещения зоны DNS, интегрированной с Active Directory. Благодаря разделу приложений (Application Partition) в Windows Server 2003 она может быть размещена на всех серверах DNS домена или даже всех DNS-серверах леса. Однако эту возможность стоит использовать в более крупных сетях, к которым наша сеть пока не относится.

Проще говоря, если вы установите в филиале контроллер домена и установите на нем службу DNS, то он также станет полноправным сервером DNS, который будет обмениваться информацией DNS со своим партнером и должным образом отвечать на запросы DNS. Такой сервер будет пред-

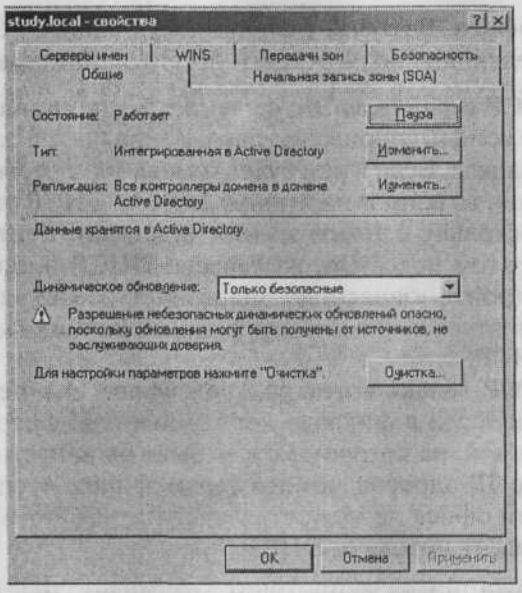


Рис. 27.2. *Диалоговое окно свойств зоны study.local*

почитаемым сервером DNS как для самого себя, так и для всех остальных компьютеров филиала.

Если в филиале нет контроллера домена, но есть сервер под управлением Windows Server 2003 (или Windows 2000 Server), то можно настроить его как вторичный сервер DNS зоны study.local. Такой сервер будет регулярно копировать данные зоны с первичного сервера, которым будет для него сервер DNS в головном офисе. Как и в предыдущем случае, этот вторичный сервер будет предпочитаемым сервером DNS как для самого себя, так и для всех остальных компьютеров филиала. Функционировать DNS в филиале будет точно так же, но данные зоны будут передаваться отдельно от процесса синхронизации активного каталога.

Если в филиале нет ни одного компьютера с серверной операционной системой, клиентским компьютерам придется обращаться к серверу DNS в центральном офисе. DNS-запросы так загрузят медленное соединение, что это сильно замедлит процесс регистрации.

27.4.2. Служба DHCP

Служба DHCP обеспечивает автоматическое назначение IP-адресов и прочих параметров настройки протокола IP клиентским компьютерам и другим сетевым устройствам, например, принтерам. Для филиала нужно выделить диапазон IP-адресов, не пересекающийся с диапазоном

центрального офиса. В случае наличия центрального офиса и филиала, существуют следующие возможности организации сервиса DHCP.

- **Сервер DHCP в филиале.** Это решение обеспечит наиболее быстрое и безопасное конфигурирование параметров протокола IP для рабочих станций филиала. Если в нем будет компьютер с серверной операционной системой, то вопрос настройки службы DHCP разрешается очень просто. Поскольку с точки зрения адресации протокола IP филиал является другой подсетью, на сервере DHCP в центральном офисе можно настроить «запасной» диапазон адресов, адреса из которого будут назначаться компьютерам филиала при отказе их собственного сервера DHCP.
- **Сервер DHCP только в центральном офисе**. Это решение актуально в том случае, если в филиале нет компьютера с серверной операционной системой, на котором можно было бы запустить сервер DHCP. Назначение IP-адресов компьютерам филиала сервером DHCP в центральном офисе не может осуществляться автоматически, нужно настроить агент передачи DHCP.

После включения, когда компьютер определит, что он настроен для автоматической адресации, он попытается установить связь с сервером DHCP. Поскольку IP-адреса у него еще нет, он не может взаимодействовать с сервером DHCP напрямую и посылает широковещательный запрос, который «слышат» все серверы DHCP, находящиеся в той же подсети. Головной офис находится в другой подсети, поэтому широковещательный запрос туда не дойдет (такие запросы не маршрутизируются). Именно поэтому нужно установить агент передачи DHCP. Этот агент пригодится и в первом случае, когда компьютерам филиала понадобится воспользоваться запасным диапазоном адресов в центральном офисе.

27.4.3. Служба WINS

В «чистой» сети, то есть в сети, где из операционных систем есть только Windows 2000/XP/2003, эта служба не нужна вообще. Если же некоторым компьютерам филиала нужно преобразовывать имена NetBIOS, то существуют две возможности:

- **Сервер WINS в филиале**. Если в филиале есть компьютер с серверной операционной системой, то службу WINS можно запустить на нем. Такой сервер зарегистрирует имена своих интерфейсов NetBIOS. Другие компьютеры филиала, настроенные на этот же сервер WINS, поступят так же, и других имен в базе данных WINS филиала не будет. Компьютеры же головного офиса регистрируют свои имена NetBIOS на собственном сервере WINS, поэтому при попытке обратиться по NetBIOS-имени к компьютеру из другого офиса возникнут проблемы.

Чтобы связь по NetBIOS-именам между офисами работала, нужно настроить репликацию между серверами WINS, которой мы займемся позже.

- **Сервер WINS в центральном офисе.** При выборе этого решения произойдет то же самое, что и с другими службами: дополнительная нагрузка на медленную линию. Компьютеры-клиенты службы WINS регистрируют свои NetBIOS-имена при каждом включении, поэтому лишний трафик будет появляться не только при обращении по NetBIOS-имени к какому-либо устройству. Оптимизацию этой нагрузки можно провести на сервере WINS, это подействует на несколько сотен компьютеров.

27.4.4. Служба сертификации

Службу сертификации невозможно запустить на нескольких компьютерах одновременно. Более того, учитывая огромную важность безопасности этой службы, администраторам хорошо было бы держать сервер под пристальным вниманием. Поскольку нам не понадобится еще один сервер сертификации в сети, мы можем оставить все без изменений.

27.5. Промежуточные итоги

Итак, мы устанавливаем в филиале собственный контроллер домена. На этот же сервере запустим службы DNS, WINS и DHCP, обслуживающие только компьютеры филиала. Зона DNS будет интегрирована в Active Directory, поэтому синхронизацию данных зоны дополнительно настраивать не придется. Мы настроим только репликацию базы WINS. На сервере DHCP в центральном офисе мы затем выделим диапазон IP-адресов, соответствующий диапазону клиентских компьютеров филиала.

27.6. Как все это организовать?

И в этом случае нам не удастся обойтись без тщательного планирования дальнейших действий. Первым важным шагом будет определение подсети, в которой компьютеры филиала получат адреса. Если их немного, мы можем выбрать, например, подсеть 192.168.20.0/24.

Следующим шагом, само собой, после тестирования только что созданного соединения, будет установка контроллера домена. Созданное подключение можно протестировать, подключив к нему компьютер и задав ему IP-адрес из диапазона подсети 192.168.20.0/24. В качестве шлюза выхода

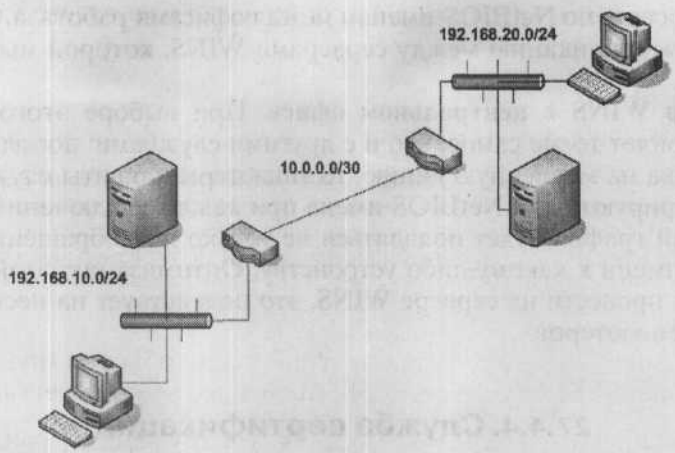


Рис. 27.3. *Пример организации двух подсетей. Подсеть 10.0.0.0/30 предоставлена поставщиком услуг связи*

укажите внутренний IP-адрес маршрутизатора, а серверы DNS и WINS задайте те же, что используют компьютеры в центральном офисе. Затем проверьте регистрацию в домене, в том числе доступность различных сетевых служб, и связь с компьютерами головного офиса (команда PING, доступ к общим папкам, доступ посредством инструментов управления к домену Active Directory и т.д.).

Примечание.

Аппаратный маршрутизатор для подключения филиала не обязателен: возможностью маршрутизации обладает операционная система Windows Server 2003. В качестве канала связи можете использовать Интернет, настроив зашифрованный туннель IP-to-IP. Единственной проблемой при использовании Интернета может стать только то, что провайдер не гарантирует пропускной способности канала.

27.6.1. Установка контроллера домена

Установка контроллера домена может быть не так проста. Если, например, между центральным офисом и филиалом у вас будет медленная связь, которая к тому же не в состоянии будет обеспечивать достаточную степень надежности, то у вас могут быть трудности. После повышения роли сервера до контроллера домена начнется репликация всей доменной базы данных размером в десятки мегабайт. В крупных сетях такая репли-

кация может занять канал соединения на несколько часов, а в крайних случаях и дней.

Примечание.

Приблизительный объем базы данных Active Directory можно определить по размеру файла NTDS.DIT и журнальных файлов EDBxxxxx.LOG. Это не точный ее объем, поскольку при удалении объектов из базы данных размер файла NTDS.DIT автоматически не уменьшается. Чтобы уменьшить размер этого файла, нужно отключиться от сети и дефрагментировать его с помощью утилиты NTDSUTIL.

Кроме доменной базы, будут скопированы также объекты групповой политики (папка SYSVOL), так что ее объем тоже нужно учесть.

Если вы предполагаете, что могут возникнуть трудности с репликацией, у вас в распоряжении есть две возможности:

- **Подготовка сервера в центральном офисе.** Повышение роли сервера до контроллера домена выполняется, когда сервер физически находится в центральном офисе. Новый сервер будет иметь до определенного времени выданный ему IP-адрес из подсети центрального офиса. Затем нужно настроить сетевые службы, провести репликацию (например, базы данных WINS) и подключить сервер к подсети филиала. Последующие шаги, которые необходимо произвести в домене Active Directory, мы рассмотрим позднее.
- **Установка контроллера домена в отключенном режиме.** Этот способ можно использовать только в системах Windows Server 2003. Он применяется, когда сервер, который станет контроллером домена, невозможно доставить в центральный офис, потому что на нем, например, запущено приложение, работу которого нельзя прерывать.

Последовательность действий по установке контроллера домена в новом филиале:

1. Подключите к сети в новом филиале «чистый» компьютер.
2. Установите на него операционную систему Windows Server 2003. В ходе инсталляции укажите, что этот компьютер будет членом домена study.local. Затем установите сервисы DHCP, WINS и DNS.
3. Настройте компьютер следующим образом:
   - Имя: SRVR003
   - IP-адрес: 192.168.20.2
   - Маска подсети: 255.255.255.0
   - Адрес сервера DNS: 192.168.10.2
   - Адрес сервера WINS: 192.168.10.2

Подготовка репликации доменной базы

В обычном случае вы по окончании настройки ввели бы команду DCPROMO, завершив таким образом повышение роли сервера до контроллера домена. Однако у нас очень медленное соединение, которое мы не хотим отягощать репликацией, поэтому проведем репликацию в отключенном режиме через архивирование.

1. Зарегистрируйтесь на SRVR001 как администратор и запустите программу архивации (NTBackup.exe).
2. На вкладке **Архивация** установите флажок **System State** и в поле **Носитель архива или имя файла** введите путь к файлу архивации (например, C:\Backup.bkf). Затем нажмите кнопку **Архивировать**.
3. В диалоговом окне **Сведения о задании архивации** нажмите на кнопку **Дополнительно**. Из раскрывающегося списка **Тип архива** выберите пункт **Копирующий**. Затем нажмите кнопку **OK** и нажатием на кнопку **Архивировать** запустите процесс архивации состояния системы.
4. Получившийся файл BACKUP.BKF запишите на диск CD, DVD или на жесткий диск компьютера SRVR003.

Инсталляция контроллера домена из архива

1. Зарегистрируйтесь на SRVR003 как администратор.
2. Запустите программу архивации и перейдите на вкладку **Восстановление и управление носителем**.
3. Щелкните правой клавишей мыши по значку **Файл** и из контекстного меню выберите команду (она там единственная) **Занести файл в каталог**. В диалоговом окне **Открытие архивного файла** введите путь к файлу BACKUP.BKF, скопированному вами с компьютера SRVR001.
4. В левом подокне инструмента **Архивация** нажмите на отображенный значок сохранённых данных и установите флажок **System State**.
5. Из списка **Восстановить файлы в** выберите **Альтернативное размещение**, а в поле **Альтернативное размещение** введите путь, по которому размещаются данные для обновления состояния системы сервера SRVR001.
6. Отобразится уведомление, что в случае смены месторасположения на альтернативное не все данные будут восстановлены. Нажмите кнопку **OK**.
7. В меню **Пуск** нажмите команду **Выполнить** и в поле **Открыть** введите команду **dcpromo /adv**. Затем нажмите кнопку **OK**.
8. В диалоговом окне **Мастер установки Active Directory** нажмите кнопку **Далее**.
9. В диалоговом окне **Совместимость операционной системы** нажмите кнопку **Далее**.

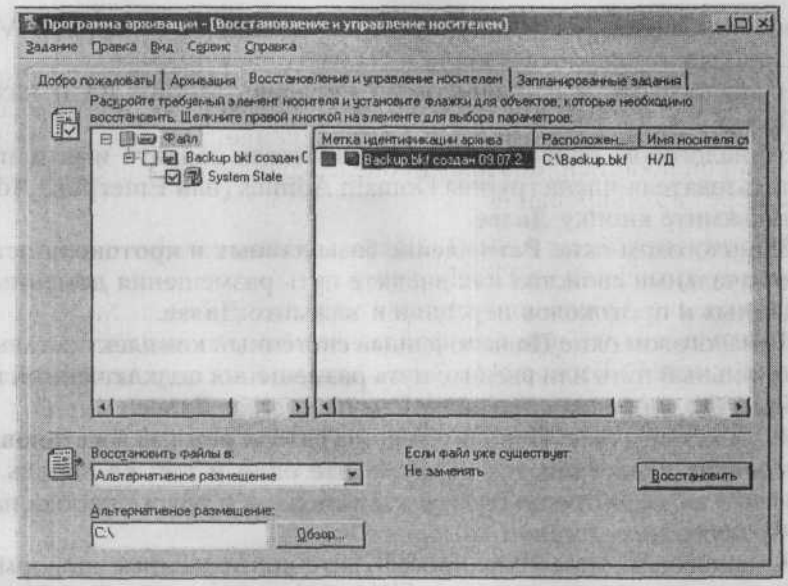


Рис. 27.4. *Восстановление архива состояния системы*

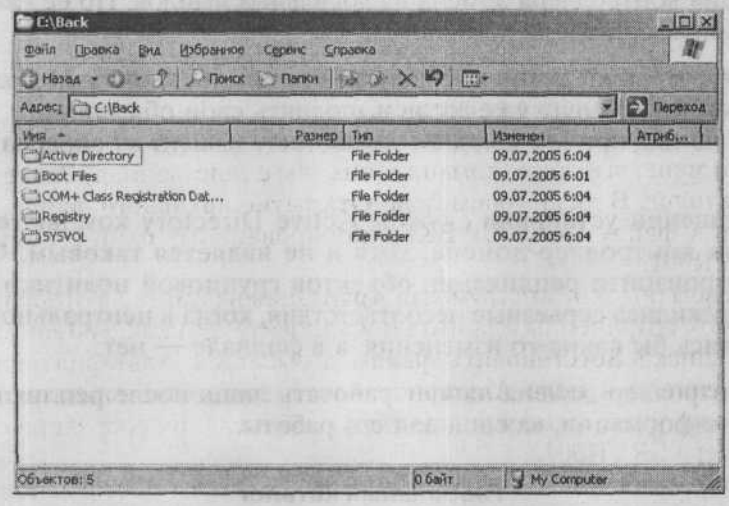


Рис. 27.5. *Содержимое папки с данными о состоянии системы*

10. В диалоговом окне **Тип управляющего доменом компьютера** отметьте **Еще один управляющий доменом компьютер для уже существующего домена** и нажмите **Далее**.
11. В диалоговом окне **Копирование информации о домене** отметьте **Из обновленных файлов сохранённых данных** и введите путь к папке с

восстановленными файлами состояния системы сервера SRVR001. Продолжите нажатием кнопки **Далее**.

12. В диалоговом окне **Глобальный каталог** ответьте **Да** и нажмите **Далее**.
13. В диалоговом окне **Сетевые пользователи** задайте имя и пароль пользователя-члена группы Domain Admins (или Enterprise Admins) и нажмите кнопку **Далее**.
14. В диалоговом окне **Размещение базы данных и протокола** оставьте изначальные свойства или введите путь размещения доменных баз данных и протоколов передачи и нажмите **Далее**.
15. В диалоговом окне **Подключенный системный комплект** оставьте изначальный путь или введите путь размещения подключенной папки SYSVOL и продолжите нажатием на кнопку **Далее**.
16. В диалоговом окне **Пароль администратора режима восстановления сервисов адресации** два раза введите один и тот же пароль и нажмите далее. Хорошо было бы задать один и тот же пароль на всех управляющих доменом компьютерах.
17. В диалоговом окне **Итог** просмотрите все введенные информации. Если вы хотите изменить что-нибудь из этого, нажмите **Назад**. В противном случае нажмите на кнопку **Далее**. Запустится инсталляция контроллера домена из локальных файлов. По ее окончании компьютер перезагрузится.

После перезагрузки компьютера может показаться, что контроллер домена в данный момент уже готов выполнять свои обязанности. Однако это пока не так, причем когда он заработает, зависит от способа инсталляции.

По завершении установки службы Active Directory компьютер везде виден как контроллер домена, хотя и не является таковым. Сначала должна произойти репликация объектов групповой политики. Потом бы обнаружились серьезные несоответствия, когда в центральном офисе проводились бы какие-то изменения, а в филиале — нет.

Итак, контроллер домена начнет работать лишь после репликации некоторой информации, важной для его работы.

Глобальный каталог

В ходе инсталляции контроллера домена мы отметили пункт, на основании которого этот сервер будет инсталлирован также как глобальный каталог. Определенно, стоит порекомендовать глобальный каталог для каждой сети.

В этом случае запрос и ответ о членстве в универсальных группах будет отработан локально, без обращения к серверу из другой подсети. Заодно

при разрыве соединения обеспечен вход пользователей. То есть если при регистрации отсутствует возможность использовать глобальный каталог, пользователь может воспользоваться профилем, размещенным в локальной памяти. Если же пользователь еще не был зарегистрирован в системе, то у него нет возможности войти в нее. Исключение составляют только члены группы Domain Admins, всегда имеющие возможность входа.

Глобальный каталог служит не только для регистрации. Он, например, упорядочивает запросы на поиск объектов в доменах Active Directory во всем лесе. Он может играть значительную роль также в соединении с другими программными продуктами (например, Exchange Server 2003).

Поскольку для регистрации пользователей из глобального каталога не используются никакие данные, кроме сведений о членстве пользователя в универсальных группах, можно на контроллере домена определить порядок размещения информации о членстве в универсальных группах в локальном кэше. В этом случае контроллер домена будет связываться с глобальным каталогом каждые 8 часов и обновлять содержимое своего кэша (до 500 универсальных групп).

Глобальный каталог — выгодная вещь, но бывают состояния, в которых невозможно обеспечить его присутствие, но все-таки нужно обеспечить быстрый и успешный вход. Не определяйте глобальный каталог в филиале в следующих случаях:

- На локальном контроллере домена стоит операционная система Windows Server 2003, разрешающая кэшировать информацию о членстве в универсальных группах.
- Оборудование контроллера домена не настолько производительно, чтобы он мог стать узлом глобального каталога.
- Соединение с филиалом медленно и ненадежно. Тогда не будет обеспечена репликация всей информации глобального каталога со всего леса.

27.6.2. Настройка сайта Active Directory

Сейчас новый контроллер домена привязан к сайту, который до сих пор был единственным — центральному офису. Репликация доменной базы проходит каждые 15 секунд, что не очень удобно. Сейчас мы организуем новый сайт и привяжем к нему компьютеры филиала по адресу подсети.

Создание нового сайта

1. Зарегистрируйтесь на PC001 как администратор (член группы Enterprise Admins), и запустите оснастку **Active Directory — сайты и службы**.

2. Раскройте объект **Sites (Сайты)**. Он содержит сайт под названием, если вы ничего не переименовывали, «Исходное название первого сайта». Контейнер **Серверы** этого сайта содержит оба контроллера домена — SRVR001 и SRVR003.
3. Из контекстного меню контейнера **Сайты** выберите команду **Новый сайт**. В диалоговом окне **Новый объект — сайт** введите в поле **Название** имя нового сайта — например, «Branch» (не используйте символов кириллицы, так как это имя будет известно в службе DNS). Затем щелкните по подключению **DEFAULTIPSITELINK** и нажмите кнопку **OK**. Переименуйте также сайт центрального офиса — например, в «MainOffice».
4. Прочитайте сообщение в окне **Active Directory** и нажмите кнопку **OK**. Новый сайт создан.

Настройка подсети

1. В консоли **Active Directory — сайты и службы** щелкните по контейнеру **Subnets (Подсети)**. В правом подокне отобразится информация об адресации существующей (пока единственной) подсети (192.168.10.0/24).
2. Из контекстного меню контейнера **Subnets** выберите команду **Новая подсеть**.
3. В диалоговом окне **Новый объект — Подсеть** введите в поле **Адрес** 192.168.20.0, а в поле **Маска** — 255.255.255.0. Затем выберите из списка сайт «Branch», к которому будет относиться эта подсеть, и нажмите **OK**.

Настройка соединения сайтов

1. В консоли **Active Directory — сайты и службы** раскройте контейнер **Inter-Site Transports** и щелкните по значку IP. В правом окне отобразится объект соединения сети под названием DEFAULTIPSITELINK.
2. Правой кнопкой мыши щелкните по этому объекту и из контекстного меню выберите команду **Переименовать**. Дайте соединению имя «MainOffice <-> Branch».
3. Из контекстного меню соединения выберите команду **Свойства**. В правой части окна свойств проверьте, что это соединение соединяет два наших сайта.
4. В поле **Повторять раз в** введите частоту репликации (например, 60 минут) и нажмите кнопку **Изменить план**. Здесь вы можете задать расписание репликации (например, оставить ее круглосуточной). Два раза нажмите кнопку **OK**.

Перемещение контроллера домена SRVR003 в новый сайт

1. В консоли **Active Directory — сайты и службы** щелкните правой кнопкой мыши по значку сервера SRVR003 и из контекстного меню выберите **Переместить**.
2. В диалоговом окне **Переместить сервер** выберите из списка сайт «Branch» и нажмите **OK**. Сервер SRVR003 перемещен, и репликация будет осуществляться ежечасно.

27.6.3. Настройка службы DNS

Чтобы служба DNS нормально работала в филиале и запросы при медленном соединении не шли бы в центральный офис, нужно проверить настройку сервиса DNS на компьютере SRVR003, затем отрегулировать параметры протокола IP на этом сервере и назначить ему IP- адрес в диапазоне сервера DHCP.

Проверка настройки DNS

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль управления DNS.
2. Правой кнопкой мыши щелкните по значку DNS и из контекстного меню выберите команду **Подключиться к серверу DNS**. В диалоговом окне **Подключиться к серверу DNS** отметьте **На компьютере** и введите SRVR003. Затем нажмите кнопку **OK**.
3. В консоли DNS раскройте объект сервера SRVR003, а затем контейнер **Зоны первоочередного поиска**. Хотя вы еще не проводили настройку, тут указана зона study.local. Все данные этой зоны входят в домен Active Directory.
4. Щелкните по значку зоны study.local и в правом подокне консоли найдите запись типа SOA (Start of Authority). Обратите внимание на серийный номер этой записи, который определяет актуальность содержания зоны. Тот же номер должен присутствовать в зоне study.local на сервере SRVR001. Это признак нормального функционирования репликации Active Directory.
5. Правой кнопкой мыши щелкните по значку зоны study.local сервера SRVR003 и отобразите ее свойства. Проверьте, что они совпадают со свойствами этой зоны на сервере SRVR001.

Параметры протокола IP на сервере SRVR003

Каждый сервер DNS должен быть сам себе клиентом. Для этого нужно изменить IP-адрес сервера DNS в свойствах подключения по локальной сети компьютера SRVR003.

1. Зарегистрируйтесь на SRVR003 как администратор.
2. Отобразите свойства подключения по локальной сети, а затем — свойства протокола TCP/IP. В поле **Предпочитаемый сервер DNS** введите адрес компьютера SRVR003 — 192.168.20.2.
3. Нажатием на кнопку **OK** закройте все диалоговые окна.

Трансляция имен Интернета

Если центральный офис организации имеет подключение к Интернету, то это же подключение захочет использовать и филиал. Однако если компьютеры филиала используют собственный сервер DNS на SRVR003, нужно, чтобы этот сервер мог решать задачу преобразования внешних имен, т.е. названий Интернета.

Поскольку мы уже настраивали это раньше, будет достаточно перенаправить неразрешенные запросы DNS с сервера SRVR003 на сервер, который сможет справиться с этой задачей. Если это сервер SRVR001, нужно в свойствах сервера SRVR003 добавить в меню **Серверы передачи** IP-адрес сервера SRVR001 (192.168.10.2).

27.6.4. Настройка службы WINS

Сервис WINS после установки не требует дополнительной настройки. Однако для нашей сети будет важно настроить репликацию между двумя серверами WINS (SRVR001 и SRVR003). Только так вы обеспечите взаимную доступность баз NetBIOS-имен в центральном офисе и филиале.

Сервер WINS должен быть сам себе клиентом. В качестве IP-адреса сервера WINS для SRVR003 в свойствах подключения по локальной сети укажите его собственный адрес (192.168.20.2). а

Настройка репликации серверов WINS

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль WINS.
2. Добавьте на консоль оба сервера WINS — SRVR001 и SRVR003.
3. Щелкните по значку сервера SRVR001. Затем правой кнопкой мыши щелкните по значку **Партнерские серверы для репликации** и из контекстного меню выберите команду **Новый партнерский сервер для репликации**. В поле **Сервер WINS** диалогового окна **Новый партнерский сервер для репликации** введите название сервера SRVR003. Затем нажмите кнопку **OK**. Стандартным типом репликации является Push/Pull.
4. Щелкните по значку **Партнерские серверы для репликации**. В правом подокне консоли WINS отобразите свойства сервера SRVR003.

На вкладке **Дополнительно** настройте параметры обоих типов репликации. Для репликации по запросу частота по умолчанию — каждые 30 минут, для репликации по предложению нет границ. В поле **Количество изменений номера версии перед репликацией** введите значение 20. Диалоговое окно свойств закройте нажатием кнопки **OK**.

5. Повторите пункты 3 и 4 для сервера SRVR003.

Репликация между серверами WINS будет проходить следующим образом. Оба они обмениваются содержанием своих баз данных каждые 30 минут. Если же у какого-нибудь сервера в течение этого интервала количество изменений перешагнет 20, то он уведомит об этом своего партнера, который тут же начнет скачивать содержание его базы данных.

Обычно нельзя рекомендовать какие-то строго определенные параметры репликации. Все всегда зависит от конкретной сети, поскольку в каждой из них иное количество компьютеров, использующих сервис WINS, и в каждой сети по-разному загружено соединение, через которое проходит репликация. Оптимизация настройки — вопрос последовательности исполнения функций сетью и необходимых измерений.

27.6.5. Настройка службы DHCP

В этом параграфе мы проведем настройку службы DHCP так, что в филиале будет собственный сервер DHCP и в центральном отделе — страховка на случай, если сервер филиала будет недоступен.

Для этого шага нужно разделить подсеть, в которой имеют адреса компьютеры филиала, на две части. Обычно в таком случае наиболее удобно соотношение 80/20, причем компьютерам должно хватать 80% всей подсети.

В нашем случае, когда мы используем в филиале подсеть 192.168.20.0/24, мы можем адресовать не более 254 компьютеров. Как и в главе 3, для рабочих станций отведем диапазон адресов от 192.168.20.17 до 192.168.20.254. Разделив эти 238 адресов в отношении 80/20, получим 190/48. Если мы не планируем в филиале более 190 компьютеров, все в порядке; иначе нужно соотношение адресов или назначить филиалу другую подсеть (с более короткой маской подсети).

Сервер DHCP филиала будет выдавать компьютерам адреса от 192.168.20.17 до 192.168.20.206. А сервер в центральном отделе будет выдавать компьютерам адреса от 192.168.20.207 до 192.168.20.254.

Настройка сервера в филиале

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль DHCP.

2. Добавьте в консоль сервер SRVR003. Из контекстного меню сервера srvr003.study.local выберите команду **Создать область**. По этой команде запустится Мастер создания области. Нажмите **Далее**.
3. В диалоговом окне **Имя области** введите название области (например, «Branch») и ее описание. Нажмите **Далее**.
4. В диалоговом окне **Диапазон IP-адресов** введите в поле **Начальный IP-адрес** первый незанятый адрес в вашей подсети (например, 192.168.20.17), а в поле **Конечный IP-адрес** — значение 192.168.20.206. Поля маски будут заполнены по умолчанию текущей маской сети (в нашем случае 24\255.255.255.0). Нажмите **Далее**.
5. В диалоговом окне **Добавление исключений** оставьте все значения пустыми и нажмите **Далее**.
6. В диалоговом окне **Срок действия аренды адреса** оставьте значение по умолчанию и нажмите **Далее**.
7. В диалоговом окне **Настройка параметров DHCP** выберите **Да, настроить эти параметры сейчас** и нажмите **Далее**.
8. В диалоговом окне **Маршрутизатор (основной шлюз)** введите адрес 192.168.20.1 (адрес маршрутизатора, передающего пакеты в главный офис). Нажмите **Далее**.
9. В диалоговом окне **Имя домена и DNS-серверы** введите в поле **Родительский домен** «study.local», а в поле **IP-адрес** введите адрес 192.168.20.2 и 192.168.10.2. Нажмите **Далее**.
10. В диалоговом окне **WINS-серверы** введите адреса 192.168.20.2 и 192.168.10.2. Нажмите **Далее**.
11. В диалоговом окне **Активировать область** отметьте **Да** и нажмите **Далее**.

Сервер DHCP настроен, однако пока не будет выдавать адреса IP и прочие параметры. Сначала необходимо авторизовать его в домене Active Directory.

Авторизация сервера DHCP в Active Directory

1. Зарегистрируйтесь на сервере SRVR001 как член группы Enterprise Admins и запустите консоль DHCP.
2. В левой части окна консоли щелкните правой кнопкой мыши по srvr003.study.local и из контекстного меню выберите команду **Авторизовать**. Обновите окно консоли, и у сервера появится зеленый значок. Если сервер все еще отображается как неавторизованный, перезапустите консоль DHCP.

Настройка сервера DHCP в центральном офисе

При конфигурации сервера DHCP в центральном отделе действуйте так же, как при настройке сервера DHCP филиала. Создайте еще одну

область, с диапазоном адресов IP от 192.168.20.207 до 192.168.20.254 с такими же возможностями.

Если сейчас, сразу после настройки запасного диапазона, сервер DHCP филиала прекратит работу, клиенты из филиала еще не готовы получать адреса от сервера SRVR001: широковещательный запрос не пройдет через маршрутизатор. Необходимо настроить агент передачи DHCP.

Агент передачи DHCP должен работать на интерфейсе, способном получать широковещательные запросы, то есть на внутреннем интерфейсе компьютера SRVR003 (это замечание на тот случай, если сетевых интерфейсов несколько).

Связь компьютеров в центральном офисе

Поскольку в центральном отделе был настроен доступ в Интернет, у всех компьютеров, желающих его использовать, адрес шлюза выхода настроен на компьютер, осуществляющий подключение. Это значит, они не смогут поддерживать связь с компьютерами филиала.

Шлюз выхода — компьютер, на который будут отосланы различные пакеты, которые неясно, куда отсылать. У него есть информация о пакетах, предназначенных для компьютеров локальной сети, остальные же пакеты он отсылает серверу SRVR002. Это подходящая ситуация, если мы будем настраивать связь в направлении филиала: будет достаточно настроить ее в одном компьютере, и он, в свою очередь, передаст ее маршрутизатору.

Предположим, что внутренний интерфейс маршрутизатора (предоставленного поставщиком услуг связи) имеет IP-адрес 192.168.10.3. Для сервера SRVR002, как и для остальных компьютеров, в качестве адреса шлюза выхода указан 192.168.10.1. Все пакеты, предназначенные во внешний мир, SRVR002 отсылает на этот адрес, а шлюз отправляет их со своего внешнего интерфейса в Интернет. Но филиал — не внешний мир, и пакеты, предназначенные для него (для подсети 192.168.20.0/24), нужно передавать маршрутизатору192.168.10.3. Это настроить просто:

1. Зарегистрируйтесь на SRVR002 как администратор.
2. В командной строке введите следующую команду:

```
route -p add 192.168.20.0 mask 255.255.255.0 192.168.10.3
```

Команда значит, что все пакеты, отправленные на адрес из подсети 192.168.20.0/24, будут переданы на адрес 192.168.10.3. Ключ -p к тому же обеспечивает постоянную запись этого маршрута в системный реестр компьютера, так что маршрут доступен и после перезагрузки.

Настройка агента передачи DHCP

1. Зарегистрируйтесь на SRVR003 как администратор и запустите оснастку **Маршрутизация и удаленный доступ**.
2. Если эта служба не запущена, из контекстного меню сервера SRVR003 выберите команду **Настроить и разрешить маршрутизацию и удаленный доступ**. Запустится Мастер установки. Нажмите **Далее**.
3. В диалоговом окне **Настройка** установите флажок **Собственные настройки** и нажмите **Далее**.
4. В диалоговом окне **Собственные настройки** установите флажок **Маршрутизация локальной сети (LAN)** и нажмите **Далее**.
5. Завершите работу Мастера нажатием кнопки **Готово** и запустите службу маршрутизации, нажав кнопку **Да**.
6. Разверните список **Маршрутизация IP** и правой кнопкой мыши щелкните по значку **Общие**. Из контекстного меню выберите команду **Новый протокол маршрутизации**. Выберите **DHCP Relay Agent** и нажмите **OK**.
7. Под значком **Маршрутизация IP** теперь добавится значок **Агент передачи DHCP**. Щелкните по нему правой кнопкой мыши и из контекстного меню выберите команду **Новый интерфейс**. В диалоговом окне **Новый интерфейс** выберите интерфейс подключения к локальной сети и нажмите **OK**.
8. В диалоговом окне свойств определите время, после которого агент передачи начнет работу (можете оставить изначальные 4 секунды) и нажмите кнопку **OK**.
9. Отобразите свойства **Агента передачи DHCP**.
10. В поле **Адрес сервера** введите IP-адрес сервера DHCP в центральном офисе (192.168.10.2) и затем нажмите на кнопки **Добавить** и **OK**.

27.6.6. Настройка глобального каталога

При инсталляции роли контроллера домена на сервер SRVR003 мы указали, что этот компьютер будет сервером глобального каталога. Поскольку иногда будет необходимо лишить его функций сервера глобального каталога, мы рассмотрим то место, где глобальный каталог настраивается.

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль **Active Directory — сайты и службы**.
2. Разверните ветвь **Branch\Servers\SRVR003** и правой кнопкой мыши щелкните по значку **NTDS Settings**.
3. Отобразится диалоговое окно свойств, в котором в разделе **Общие** будет установлен флажок **Глобальный каталог**.

Если вы хотите настроить какой-нибудь контроллер домена как узел глобального каталога, подумайте о том, что выполнять эту функцию он сможет

лишь тогда, когда у него будет копия всех необходимых данных со всего леса. Этот процесс, само собой, занимает какое-то время, причем это зависит от величины сети и скорости связи между доменами. Только по завершении репликации информация о глобальном каталоге появится в зоне DNS, и компьютеры смогут начать ее использовать. К тому же нужно иметь в виду, в случае конфигурации глобального каталога, что на излишнюю репликацию в вашем домене может повлиять администратор другого домена, который, например, за один раз создаст сотни учетных данных пользователей.

Если вы выясните, что не в ваших силах удерживать на данном управляющем доменом компьютере роль глобального каталога, но у вас в сети нет другого глобального каталога, нужно хотя бы обеспечить быстрый вход пользователей. Это, само собой, касается лишь доменов в режиме Windows 2000 native или выше.

Настройка кэширования членства в универсальных группах

1. Зарегистрируйтесь на PC001 как администратор и запустите консоль **Active Directory — сайты и службы**.
2. Щелкните по значку сайта, для которого вы хотите настроить кэширование, и затем отобразите в правом окне свойства объекта **NTDS Site Settings**.
3. На вкладке **Настройка** установите флажок **Разрешить кэширование членства в универсальных группах** и из раскрывающегося списка выберите сайт, с которого будет скачиваться информация о членстве.
4. Закройте диалоговое окно нажатием на кнопку **OK**.

27.7. Итоги

Организация нового филиала, определенно, не может быть поводом для усиления команды администраторов домена. Однако это может быть поводом для усиления отдела поддержки пользователей, поскольку их число, определенно, вырастет. Нужно уделять достаточно времени для подготовки сети к дальнейшему расширению, в том числе нужно на ней все установить и проверить.

Компании, обеспечивающей связь с новым филиалом, для настройки маршрутизатора понадобится информация об адресации IP, которую вы будете использовать в филиале. Остальные задачи лежат на вас, как на администраторах сети.

Для каждой части сети, которая присоединена по медленной линии, неплохо было бы иметь отдельный сайт Active Directory. Сайт обеспечивает пользователям регистрацию в домене через контроллер, находящийся в

том же сайте, и позволяет настроить репликацию доменных данных так, чтобы создаваемый при этом трафик как можно меньше мешал обычной работе пользователей. В каждом сайте должны быть свои контроллер домена, сервер DNS и глобальный каталог.

Сервер глобального каталога важен в первую очередь для регистрации пользователей, а система Windows Server 2003 предоставляет возможность отделить эту часть от его прочих задач. Если вы не можете иметь в локальной сети глобальный каталог, существует возможность настроить в данной сети кэширование членства в универсальных группах.

Если вы будете использовать в филиале собственный сервер WINS, не забудьте настроить репликацию с остальными серверами. Только так вы обеспечите обмен базами данных имен NetBIOS между сайтами.

Сайт может иметь также собственный сервер DHCP. Однако если в сайте не будет отдельного сервера DHCP, и вы захотите использовать сервер DHCP центрального офиса, нужно выделить на этом сервере область, соответствующую диапазону адресов филиала, и настроить в филиале Агент передачи DHCP. Если в филиале нет ни одного сервера, нужно обратиться к поставщику маршрутизатора, чтобы разрешить маршрутизацию широковещательных запросов.

Управление окружением домена после появления ответвления никак не изменится — в наиболее часто используемой оснастке **Active Directory — Пользователи и компьютеры** это вообще никоим образом не отражается. Администраторы же домена получат еще одно задание — регулярная проверка успешности репликации между управляющими доменами компьютерами.

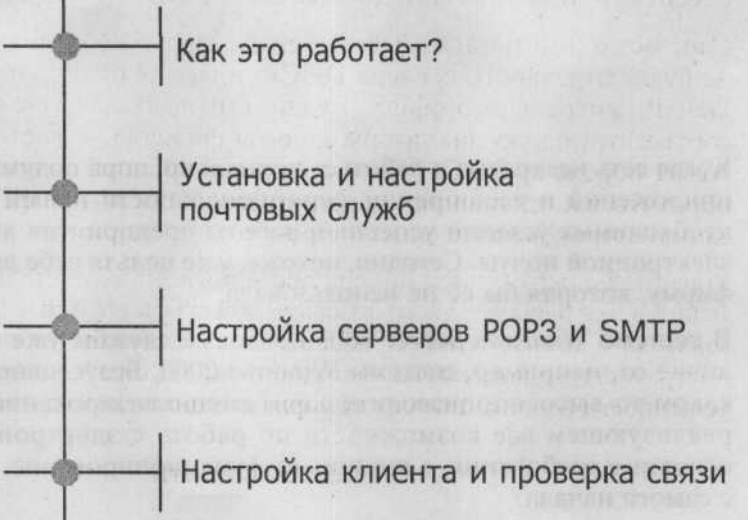
Состояние сети

В сети добавился новый филиал. В домене Active Directory он организован в сайт по имени «Branch», и в нем установлен контроллер домена SRVR003. Сеть Active Directory была отконфигурирована таким образом, что теперь предоставляет пользователям быструю регистрацию в пределах сайта. Сервер SRVR003 является теперь также сервером DNS, сервером WINS с настроенной репликацией типа Push/Pull с сервером SRVR001 и сервером DHCP с 80-процентным диапазоном адресов IP для клиентских компьютеров на ответвлении.

Чтобы в случае необходимости была возможность получить адрес IP из центрального офиса, на сервере SRVR003 был настроен агент передачи DHCP. В центральном офисе на сервере DHCP создана запасная область IP-адресов.

Репликация между контроллерами домена в центральном отделе и филиале проходит по протоколу IP ежечасно круглосуточно. Сервер SRVR003 является сервером глобального каталога.

Глава 28 Настройка службы электронной почты



Когда сеть настроена и работает нормально, пора подумать об установке приложений и расширении функциональности нашей сети. Одним из необходимых условий успешной работы предприятия является наличие электронной почты. Сегодня, похоже, уже нельзя себе даже представить фирму, которая бы её не использовала.

В системе Windows Server 2003 почтовые службы уже включены, в отличие от, например, системы Windows 2000. Безусловно, речь не идёт о каком-то высокопроизводительном специализированном приложении, реализующем все возможности по работе с электронной почтой, но основные требования, а именно, ее функционирование, выполнимы уже с самого начала.

Это значит, что вам в таком случае не нужно будет докупать дополнительные продукты или лицензии, то есть расходы на электронную почту можно свести к минимуму.

28.1. Как это работает?

Огромное количество Интернет-провайдеров предоставляет своим клиентам помимо всего прочего и почтовый ящик. Или бесплатно, или за минимальную сумму.

По такому же принципу работают и почтовые службы Windows Server 2003. Они не являются обязательными компонентами системы, и если вы хотите с ними работать, вам нужно будет установить их отдельно. Именно поэтому о подобных возможностях системы Windows Server 2003 большинство пользователей так никогда и не узнают.

Почтовая служба Windows Server 2003 работает по протоколу POP3 (Post Office Protocol), который является стандартным средством Интернета для обеспечения доступа к почтовому ящику. Он используется в Интернете с самого начала и значительно превосходит другие протоколы доступа (IMAP, HTTP).

POP3 — это протокол, позволяющий считывать информацию из почтового ящика. Для отсылки почты он не предназначен. Почта отправляется по протоколу SMTP (Simple Mail Transfer Protocol), простота которого заявлена уже в самом названии.

В ОС Windows Server 2003 каждый из названных протоколов обслуживают так называемые виртуальные серверы. Они могут быть установлены как на одном и том же физическом сервере, так и на разных. Функция сервера POP3 заключается в том, чтобы доставить почту из почтового ящика на рабочую станцию пользователя, а сервера SMTP — в том, чтобы передать сообщение, созданное на рабочей станции, в почтовый ящик или другому серверу SMTP.

28.2. Установка и настройка почтовых служб

Установка почтовых служб включает несколько шагов:

- Планирование службы электронной почты.
- Установка службы электронной почты.
- Настройка серверов POP3 и SMTP.
- Создание почтовых ящиков тестовых пользователей.
- Проверка связи.
- Создание почтовых ящиков для остальных пользователей.

28.2.1. Планирование службы электронной почты

Одним из самых важных шагов является назначение имени домену электронной почты (часть почтового адреса, следующая за символом @). Для коммуникации внутри сети этого не требуется, но для обмена сообщениями по Интернету без него не обойтись, поэтому нужно выбрать имя, действительное в глобальной сети.

Следующий шаг — это выбор почтового сервера. На нём будут установлены все почтовые ящики пользователей вашего предприятия, поэтому следует выбрать такой сервер, на котором будет для этого достаточно места и который не будет слишком отягощён стандартными функциями. Кроме того, следует помнить, что этот сервер окажется доступен извне, поэтому с точки зрения безопасности особо важные данные или приложения держать на нем не следует.

Чтобы получить доступ к своему почтовому ящику, пользователь должен быть авторизован почтовым сервером. Если почтовый сервер является рядовым сервером в домене, существуют три возможности авторизации: через доменную учетную запись пользователя, локальную учетную запись или с помощью зашифрованного пароля, хранящегося в файле. Если почтовый сервер установлен на контроллере домена, то доступ к нему через локальную учетную запись невозможен.

Сервер SMTP следует настроить так, чтобы предотвратить несанкционированную пересылку через него сообщений посторонних пользователей извне.

В нашей сети имеется три сервера: контроллеры домена **SRVR001** и **SRVR003** и рядовой сервер **SRVR002**. Для установки почтового сервера выберем **SRVR001**. Поскольку в дальнейшем нам нужно будет получать почту из Интернета, то имя домена электронной почты должно соответствовать правилам, принятым в глобальной сети. Суффикс `local` в Интернете недействителен, поэтому выберем имя study.com (предполагая, что это имя ещё не занято и мы готовы зарегистрировать его и платить за его использование).

28.2.2. Установка служб электронной почты

Для установки служб электронной почты:

1. Зарегистрируйтесь на **SRVR001** как администратор.
2. Запустите апплет панели управления **Установка и удаление программ** и выберите **Установка компонентов Windows**.
3. В диалоговом окне **Мастер компонентов Windows** отметьте поле **Службы e-mail** и нажмите кнопку **Состав**. Потом поставьте флажок **Служба POP3** (при этом будет установлен также протокол SMTP) и подтвердите нажатием на **OK**. Продолжите установку, нажав **Далее**.
4. Начнётся установка протоколов POP3 и SMTP. В процессе инсталляции вас могут попросить вставить установочный компакт-диск Windows Server 2003.
5. По окончании установки перезагружать сервер не нужно.

Вместе со службой POP3 будет установлена и консоль управления ею, которую вы найдете среди утилит администрирования на сервере **SRVR001**. Этим инструментом можно пользоваться только с того компьютера, где установлена служба POP3. Для удаленного управления почтовыми ящиками необходим веб-интерфейс, который можно было установить, выбрав компонент Web Administration, но возможность удаленного доступа снижает безопасность почты. Мы рекомендуем веб-интерфейс не устанавливать, а настраивать почтовые ящики непосредственно с сервера **SRVR001** или подключившись к удалённому рабочему столу.

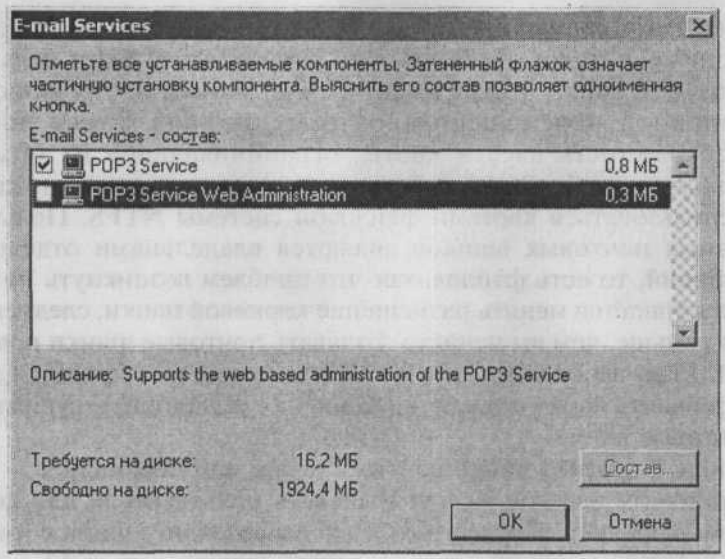


Рис. 28.1. *Состав служб e-mail*

28.3. Настройка серверов POP3 и SMTP

28.3.1. Сервер POP3

Настройка сервера POP3 производится следующим образом:

1. Зарегистрируйтесь на **SRVR001** как администратор и запустите консоль **Служба POP3**.
2. Щелкните правой кнопкой мыши по серверу и из контекстного меню выберите команду **Свойства**.
3. В диалоговом окне **Свойства** сервера POP3 убедитесь, что в поле **Метод проверки подлинности** выбрано значение **Интегрированный в Active Directory**.
4. Далее убедитесь, что в остальных полях стоят значения по умолчанию. Порт протокола TCP сервера POP3 — 110, а в поле **Уровень ведения журнала** указана только журнализация ошибок (**Минимальный**). Если вы хотите протоколировать больше информации, вы можете сменить эту установку на вариант **Средний** (записываться будут предупреждения и ошибки) или **Полный**.
5. Важным параметром является **Корневая папка почты**. Речь идёт о папке, в которой будут храниться почтовые ящики пользователей. Её с точки зрения безопасности и лучшей работы следует поместить на физический диск, свободный от системных папок (это пригодится в случае получения пользователями очень больших сообщений).

Есть два ограничения: нельзя выбрать в качестве почтовой папки корневой каталог диска (то есть указать адрес C:) и нельзя поместить ее в папке, файлы из которой на момент настройки открыты. Причиной перемещения почтовых ящиков может послужить необходимость ввести квоты, ограничивающие их объём. Поскольку служба POP3 собственных квот не имеет, нужно будет воспользоваться квотами файловой системы NTFS. Пользователи данных почтовых ящиков являются владельцами отдельных сообщений, то есть файлов, так что проблем возникнуть не должно. Если придётся менять размещение корневой папки, следует сделать это раньше, чем вы начнёте создавать почтовые ящики пользователей. Если вы сделаете это позже, то потом вам придётся вручную переносить папку с именем домена и ее подпапки — существующие почтовые ящики.

6. В поле **Корневая папка почты** оставьте исходный адрес.
7. Установите флажок **Всегда создавать пользователя для новых почтовых ящиков**. После этого, если вы создадите ящик с именем, не соответствующим ни одному из регистрационных имён, вам нужно будет ввести пароль, и в домене Active Directory появится учётная запись пользователя.
8. О поле требования безопасной проверки пароля речь будет идти дальше.

28.3.2. Домены POP3 и SMTP

До того как создать первый почтовый ящик, нам нужно будет определить имя почтового домена, которое служит двум целям:

- Определяет электронный адрес пользователя.
- Является частью регистрационного имени пользователя.

Если вы настраиваете почту для переписки не только внутри предприятия, но и в Интернете, то следует выбрать имя согласно правилам, принятым в глобальной сети, и зарегистрировать его в организации, уполномоченной выдавать доменные имена. В качестве примера мы используем имя study.com, которое в действительности давно занято.

Создание домена study.com

Чтобы создать домен `study.com`:

1. Зарегистрируйтесь на **SRVR001** как администратор и запустите консоль **Служба POP3**.
2. Щелкните правой кнопкой мыши по серверу и из контекстного меню выберите команду **Создать → Домен**.

3. В диалоговом окне **Добавить домен** в поле **Имя домена** введите имя `study.com` и нажмите **OK**. Новый домен отобразится под сервером POP3.

Теперь инфраструктура электронной почты готова, и можно начать создавать почтовые ящики.

Примечание.

После создания домена следует создать папку с тем же названием в корневой папке почты, а затем — домен локального типа в протоколе SMTP, который служит для того, чтобы сообщения, адресованные местным пользователям, не покидали локальной сети.

Почтовые ящики

1. Зарегистрируйтесь на **SRVR001** как администратор и запустите консоль **Служба POP3**.
2. Щелкните правой кнопкой мыши по домену `study.com` и из контекстного меню выберите команду **Создать → Почтовый ящик**.
3. В диалоговом окне **Добавление почтового ящика** в поле **Имя** введите регистрационное имя своей доменной учётной записи (например, `ITManager1`). Остальные поля оставьте пустыми. Снимите флажок **Создать пользователя для этого почтового адреса** и нажмите **OK**.

Начнется поиск в активном каталоге учетной записи с таким именем. Когда она будет найдена, будет сразу же создан почтовый ящик (рис. 28.3). Если учетная запись не найдена, то будет выведено сообщение об ошибке.

Чтобы сразу же проверить, как работает почтовая служба, создайте почтовый ящик по крайней мере для ещё одного пользователя (например, `Shop1`).

28.3.3. Сервер SMTP

Поскольку протокол SMTP очень прост, некоторые могут подумать, что настраивать его не нужно. Напрасно. Так как ваш SMTP-протокол будет использоваться для отправки сообщений в том числе и через Интернет, следует понять необходимость настроек, связанных с безопасностью, и смириться с тем, что сообщения при передаче никак не шифруются.

1. Зарегистрируйтесь на **SRVR001** как администратор и запустите консоль **Диспетчер служб IIS**.
2. Щелкните правой кнопкой мыши по значку **Виртуальный SMTP-сервер по умолчанию** и отобразите его свойства.

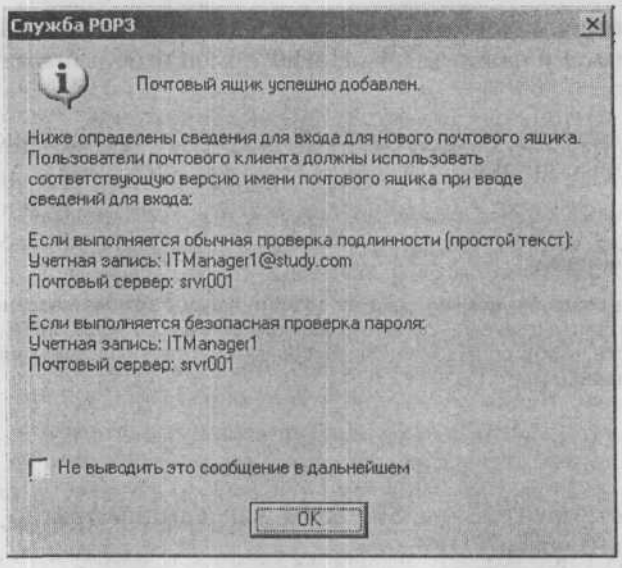


Рис. 28.3. *Почтовый ящик успешно создан*

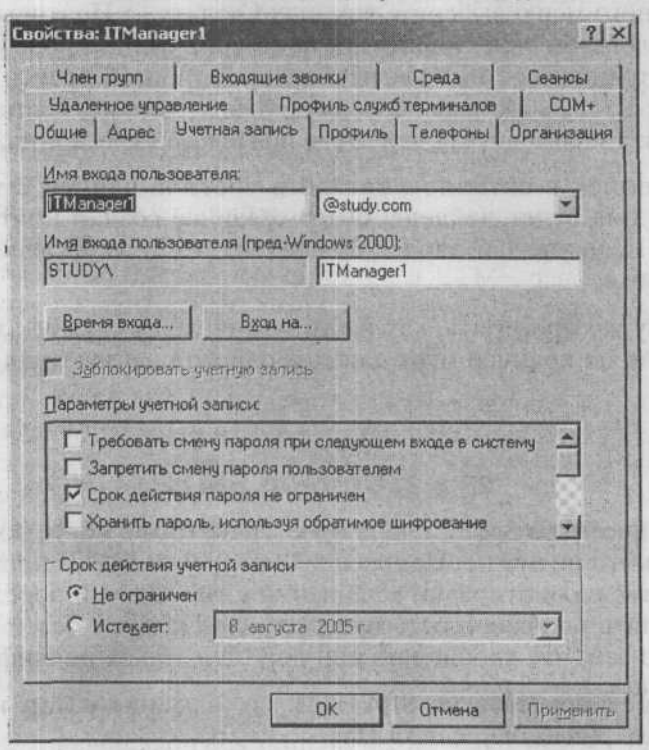


Рис. 28.4. *После создания почтового ящика регистрационное имя пользователя изменилось*

3. На вкладке **Общие** установите флажок **Вести журнал** и выберите **Расширенный формат файла журнала W3C**. Затем нажмите кнопку **Свойства**.
4. В диалоговом окне **Свойства протоколирования** отметьте поле **Использовать местное время в имени файла**. На вкладке **Дополнительно** отметьте поля **Дата, Время, IP-адрес клиента, Имя пользователя, Имя службы, Состояние протокола, Передано байт, Заняло времени** и **Версия протокола.** Закройте диалог свойств протоколирования нажатием **OK**.
5. На вкладке **Доступ** настройте (или согласитесь с предложенными настройками) следующие возможности:
   - В разделе **Управление доступом** нажмите кнопку **Проверка подлинности** и в появившемся диалоге проверки подлинности в разделе **Выбор методов проверки подлинности для ресурса** убедитесь, что выбран вариант **Анонимный доступ**. Это значит, что авторизации отправителя сообщений не требуется. Поскольку ваш сервер должен быть доступен извне, разрешить анонимный доступ необходимо, иначе вы не сможете получать сообщения.
   - В разделе **Управление подключением** можно определить, с каких IP-адресов можно подключиться к серверу. Эта настройка служит для защиты сервера, поскольку те IP-адреса, с которых доступ не разрешён, сервер SMTP обслуживать не будет. Таким образом вы можете блокировать приём нежелательных сообщений (спама) — для этого нужно знать IP-адреса тех серверов, с которых приходят такие сообщения, и постоянно пополнять список.
   - Раздел **Ограничение ретрансляции** служит для указания тех IP-адресов, которым разрешено использовать этот виртуальный сервер SMTP в качестве ретранслятора. Если разрешить пересылку почты через данный сервер от кого угодно и кому угодно, то рано или поздно этой возможностью воспользуются спамеры, наш IP-адрес попадет в черные списки и другие почтовые серверы откажутся принимать с него сообщения, в результате чего предприятие останется без исходящей почты. Локальные пользователи должны иметь возможность отсылать почту в любой домен, и это соответствует настройке по умолчанию: сервер SMTP принимает только сообщения, адресованные в его домен, а отправляет вовне только сообщения от зарегистрированных пользователей вне зависимости от их IP-адреса. Для повышения безопасности можно установить ограничение и на IP-адреса, разрешив отправку почты только с адресов вашей локальной сети и запретив со всех остальных. Однако если пользователи собираются посылать сообщения через ваш сервер извне сети (например, подключаясь к Интернету из дома), то такая настройка невозможна, потому что нельзя

предсказать, какой IP-адрес будет выделен пользователю провайдером на каждый сеанс связи. Единственным исключением, когда ограничение на IP-адреса будет уместно, является работа в виртуальной частной сети, рассмотренной в главе 26. Ограничение ретрансляции — это одна из важнейших возможностей сервера SMTP, и ей следует постоянно уделять внимание. Для того, чтобы отслеживать сообщения, проходящие через ваш сервер SMTP, служит журнал, который мы настроили в предыдущем пункте.

6. Перейдите на вкладку **Сообщения**. Здесь можно наложить ограничения на некоторые параметры сообщений, отсылаемых или принимаемых сервером SMTP. По умолчанию наложено ограничение на размер сообщения (2048 Кб). Для сообщений, адресованных вовне, это вполне разумное ограничение, однако, для сообщений внутри организации это излишне. Нужно найти компромисс. В поле **Копии отчетов о невозможности доставки отправлять по адресу** введите электронный адрес администратора сервера SMTP (например, `itmanager1@study.com`). Если кто-то отошлёт со-

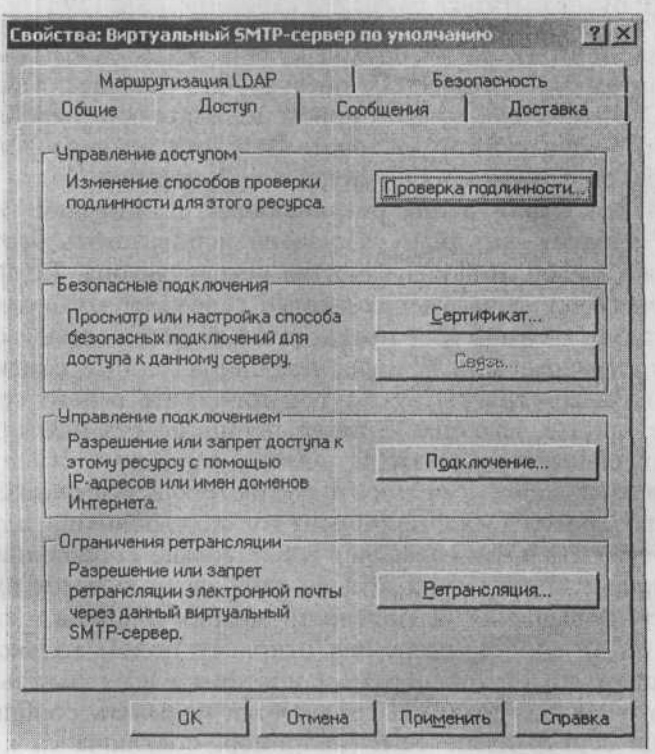


Рис. 28.5. *Вкладка Доступ в диалоговом окне свойств сервера SMTP*

общение в ваш домен на несуществующий адрес, почтовый сервер автоматически сообщит на адрес администратора о том, что сообщение не доставлено (Non Delivery Report, NDR). Таким образом, администратор сервера SMTP имеет представление обо всех сообщениях, которые были отосланы на несуществующие адреса (исходное сообщение прилагается к NDR сообщению). То же правило работает и в отношении сообщений, отправленных из вашей организации.

Примечание.

У администратора почтового сервера должен быть собственный почтовый ящик. Если уведомление о недоставке сообщения отсылать некому (например, указан несуществующий адрес), то сервер его не удалит, а поместит в папку, имя которой указано в поле **Каталог ошибочной почты**. Эту папку вам нужно регулярно просматривать и очищать.

7. Перейдите на вкладку **Доставка**. Здесь приведена информация, касающаяся отсылки электронной почты. Если пользователь пошлёт сообщение внешнему пользователю по Интернету, то сервер SMTP будет пытаться связаться с сервером SMTP домена адресата. Если этот сервер окажется временно недоступен, то сообщение будет сохранено и через некоторое время сервер снова попытается переслать его. Настройка по умолчанию требует повторить попытку через 15 минут, затем — ещё через 30, и т.д. Через 12 часов отправителю посылается уведомление о задержке сообщения,

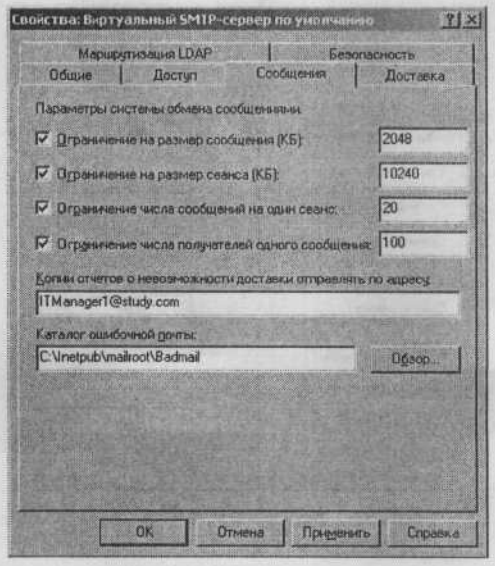


Рис. 28.6. *Вкладка Сообщения в диалоговом окне свойств сервера SMTP*

через двое суток — о том, что сообщение не доставлено (NDR). Когда пользователь из внутреннего домена посылает сообщение на адрес somebody@somewhere.com, сервер SMTP по умолчанию пытается передать это сообщение своему «коллеге», обслуживающему домен somewhere.com. Для этого он ищет в службе DNS запись типа MX (Mail Exchange). Этот путь передачи можно изменить. Например, некоторые фирмы пересылают всю свою почту через один компьютер, который проверяет её на вирусы, добавляет к каждому сообщению реквизиты компании и отсылает по указанному адресу. Если вы хотите установить такой порядок, то на вкладке **Доставка** нажмите кнопку **Дополнительно** и в поле **Направляющий узел** введите в квадратных скобках адрес вышестоящего сервера SMTP. Другая возможность — это отправлять сообщения через своего Интернет-провайдера, с которым обмен сообщениями происходит быстрее, чем с кем бы то ни было (если SMTP-сервер провайдера настроен так, чтобы разрешить ретрансляцию с вашего адреса).

Теперь серверная часть готова. Чтобы использовать её службы, нужно иметь клиента протокола POP3. Таких клиентов разработано великое множество, но традиционно используется почтовый клиент Outlook Express, входящий в состав ОС Windows 2000/XP/2003. Он вполне подходит для наших целей, а поскольку он является частью операционной системы, то его не нужно устанавливать отдельно и затраты на его поддержку окажутся минимальны.

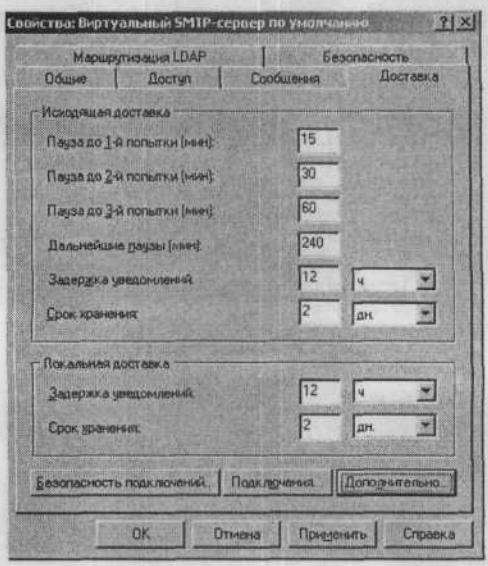


Рис. 28.7. *Вкладка Доставка в диалоговом окне свойств сервера SMTP*

28.4. Настройка клиента и проверка связи

Процедура настройки клиента Outlook Express системы Windows Server 2003 достаточно проста, чтобы доверить ее выполнение пользователям. Администратор и не сможет этого сделать, потому что почтовые настройки, индивидуальные для каждого пользователя, хранятся в пользовательском профиле. Некоторые параметры приложений Internet Explorer и Outlook Express можно настроить с помощью утилиты Internet Explorer Administration Kit (IEAK), но в общем случае пользователь должен настраивать свой почтовый клиент самостоятельно в следующем порядке:

1. Зарегистрируйтесь на **PC001** под пользовательской учетной записью.
2. Из главного меню запустите приложение Outlook Express. Откроется Мастер подключения к Интернету. В поле **Имя** введите своё регистрационное имя (`ITmanager1`) и нажмите **Далее**.
3. В диалоговом окне **Адрес электронной почты** задайте свой адрес `itmanager1@study.com`. Продолжите нажатием на кнопку **Далее**.
4. В диалоговом окне **Серверы электронной почты** введите в поля **Сервер входящих сообщений** и **Сервер исходящих сообщений** имя сервера **SRVR001**. Нажмите **Далее**.
5. В следующем диалоговом окне введите в поле **Учётная запись** своё регистрационное имя в почтовом домене (`itmanager1@study.com`), а в поле **Пароль** введите пароль учётной записи `itmanager1`. Флажок **Запомнить пароль** оставьте установленным и нажмите **Далее**.
6. В диалоговом окне **Поздравляем** нажмите **Готово**. Учётная запись электронной почты создана.

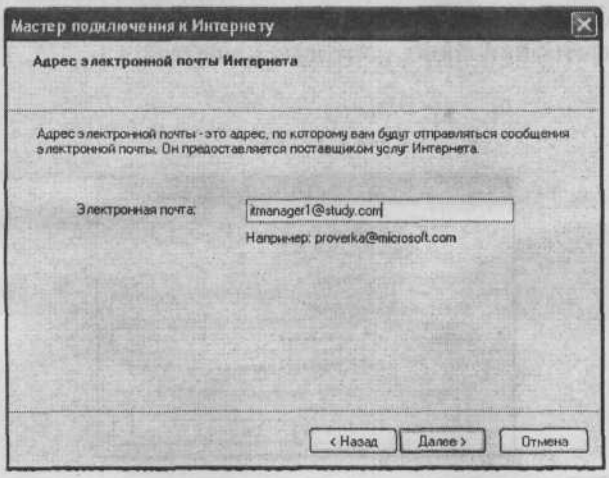


Рис. 28.8. *На этот адрес будут приходить ответы на отправленные сообщения*

Теперь вы можете проверить работу электронной почты. Создайте новое сообщение и отошлите его самому себе. Вы должны сразу же получить это сообщение после нажатия на кнопку **Доставить почту**. Отослать почту на внешний адрес у вас не получится, поскольку для этого нужно настроить разрешения.

1. В строке меню приложения Outlook Express выберите **Сервис** → **Учётные записи**.
2. В диалоговом окне **Учётные записи в Интернете** перейдите на вкладку **Почта**, выберите только что созданную учётную запись и нажмите на кнопку **Свойства**.
3. В диалоговом окне свойств подключения перейдите на вкладку **Серверы** и в части **Сервер исходящей почты** отметьте **Проверка подлинности пользователя** (рис. 28.9).

Теперь почтовый клиент будет вместе с сообщением посылать серверу SMTP свое имя и пароль, а сервер SMTP нужно настроить для их обработки.

1. Зарегистрируйтесь на **SRVR001** как администратор и запустите консоль **Диспетчер служб IIS**.
2. Щелкните правой кнопкой мыши по значку **Виртуальный SMTP-сервер по умолчанию** и отобразите его свойства.
3. На вкладке **Доступ** нажмите кнопку **Проверка подлинности** и отметьте поле **Обычная проверка подлинности**. На вопрос о передаче паролей в незашифрованном виде ответьте **Да**.

Теперь снова попытайтесь отослать сообщение на внешний адрес. Всё должно быть в порядке. Когда вы добьетесь того, чтобы два тестовых пользователя смогли обмениваться сообщениями, можно приступать к созданию почтовых ящиков для остальных пользователей и объяснению им порядка настройки своих почтовых клиентов.

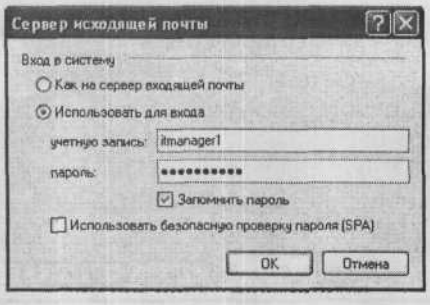


Рис. 28.9. *Настройка аутентификации пользователя для отправки сообщений*

28.5. Итоги

Система Windows Server 2003 является первой системой из семейства систем Microsoft со встроенной поддержкой электронной почты. Установку компонентов, реализующих службу электронной почты, нужно тщательно спланировать. Нужно учитывать, что пользователи могут отправлять в почтовые ящики большое количество данных, которые могут занять много места на диске, поэтому почтовые ящики следует разместить отдельно от файлов операционной системы — желательно на отдельном физическом диске.

Почтовую службу реализуют два компонента — серверы POP3 и SMTP. Протокол POP3 служит для получения сообщений из почтового ящика, протокол SMTP — для передачи сообщений, подготовленных в почтовом клиенте, в качестве которого можно использовать встроенную программу Outlook Express.

Если вы собираетесь использовать службу электронной почты для обмена сообщениями не только в пределах локальной сети, но и с внешними адресатами, то кроме настройки серверов вам нужно выполнить следующие действия:

- Выбрать имя почтового домена согласно правилам, принятым в Интернете (`study.com`), и зарегистрировать его в уполномоченной организации.
- В файл зоны DNS добавить запись типа MX, ведущую на сервер `mail.study.com`, и запись типа A, ведущую на внешний IP-адрес почтового сервера вашего провайдера.
- На сервере, обеспечивающем доступ в Интернет (**SRVR002**), настроить маршрутизацию на порт 25 сервера SMTP во внутренней сети.

Поскольку оба протокола очень просты, следует уделить внимание настройке их безопасности. Это касается как передачи паролей к учетным записям, так и самих передаваемых сообщений.

Состояние сети

В сети появилась служба электронной почты, установленная на сервере SRVR001. Созданы почтовые ящики для всех пользователей. У пользователей настроен почтовый клиент, в качестве которого выбран Outlook Express. Сервер SMTP настроен для отправки сообщений не только на внутренние, но и на внешние адреса, безопасность протокола POP3 обеспечена проверкой пароля.

Издательство «Наука и Техника»

высылает книги почтой

М.В. Антоненко,
В.В. Пономарев,
А.В. Куприянова

«Толстый» самоучитель работы на компьютере

ISBN: 5-94387-221-3
Размер: 165x235
Объем: 544 с.: ил., цв. вклейки

Эта книга — превосходный практический самоучитель, который позволяет освоить работу на компьютере «с нуля», без каких-либо предварительных компьютерных навыков. Здесь вы найдете всю необходимую информацию: как правильно обращаться с компьютером и настраивать его, как работать с Windows XP, Word и Excel, как смотреть видео и слушать музыку на ПК. Вы научитесь работать с файлами и папками, создавать и распечатывать документы, устанавливать и запускать программы, защищать компьютер от вирусов, а также многому другому. Отдельная часть книги посвящена работе в Интернете и электронной почте.

Кроме того, в книге рассмотрены такие актуальные вопросы, как: работа с цифровым фотоаппаратом (как подключить его к компьютеру, перенести и немного подредактировать фотографии), запись CD и DVD, автоматический перевод текстов с иностранных языков на русский и с русского на иностранные (вы с легкостью можете поручить это компьютеру — ничего сложного здесь нет) и др. В конце книги приведен словарик компьютерных терминов.

Книга написана в дружелюбной форме, простым и доступным языком, с большим количеством наглядных иллюстраций. Лучший выбор для начинающих.

серия — ПРОСТО О СЛОЖНОМ — серия