АЛЕКСАНДР ПОЛЯК–БРАГИНСКИЙ

АДМИНИСТРИРОВАНИЕ СЕТИ

НА ПРИМЕРАХ

ОРГАНИЗАЦИЯ РАБОТЫ СИСТЕМНОГО АДМИНИСТРАТОРА

СТАНДАРТНЫЕ И НЕСТАНДАРТНЫЕ ПРИЕМЫ АДМИНИСТРИРОВАНИЯ ЛВС

ПОЧТОВЫЙ СЕРВЕР, WEB–СЕРВЕР И ДРУГИЕ СЕРВИСЫ

СРЕДСТВА УДАЛЕННОГО УПРАВЛЕНИЯ СЕРВЕРОМ

ИСПОЛЬЗОВАНИЕ МОБИЛЬНОЙ СВЯЗИ ДЛЯ ОПОВЕЩЕНИЯ АДМИНИСТРАТОРА О СОСТОЯНИИ СЕТИ

bhv

Александр Поляк-Брагинский

АДМИНИСТРИРОВАНИЕ СЕТИ

НА ПРИМЕРАХ

Санкт-Петербург
«БХВ-Петербург»
2005

УДК 681.3.06
ББК 32.973.202
П54

Поляк-Брагинский А. В.

П54 Администрирование сети на примерах. — СПб.: БХВ-Петербург, 2005. — 320 с.: ил.

ISBN 5-94157-666-8

В доступном для начинающих системных администраторов изложении рассматриваются вопросы администрирования небольшой сети с двумя серверами Windows 2000 Server и Windows Server 2003 и рабочими станциями под управлением Windows XP и Windows 98. Изложение построено на большом количестве практических примеров. Приведено решение типичных задач администратора сети с применением стандартных и нестандартных методов, с использованием возможностей операционной системы, программ сторонних разработчиков, а также средств, созданных самим администратором. Предполагается, что читатель имеет опыт работы с компьютером на уровне опытного пользователя. Теоретические основы администрирования рассмотрены предельно кратко. Описание примеров сделано на основе реально работающей сети, что на 100% гарантирует их работоспособность при соблюдении описанных условий применения. Приведены примеры создания сценариев и программ на языках VBScript, Visual Basic и других, доступных начинающему администратору.

Для начинающих системных администраторов

УДК 681.3.06
ББК 32.973.202

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Наталья Сержантова*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн обложки	*Игоря Цырульникова*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 28.06.05.
Формат 70×100$^{1}/_{16}$. Печать офсетная. Усл. печ. л. 25,8.
Тираж 4000 экз. Заказ № 1131
"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.02.953.Д.006421.11.04 от 11.11.2004 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 5-94157-666-8

Оглавление

Введение

Одна моя знакомая сравнила роль администратора компьютерной сети в жизни организации с ролью стоматолога. Несмотря на, как правило, весьма скромное вознаграждение (в государственных структурах), в современных компьютеризированных организациях он играет роль, важность и значение которой осознаются руководителями часто лишь при возникновении кризисных ситуаций, когда под угрозой оказывается финансовое положение предприятия, его имидж на рынке или репутация руководителя в глазах более высокого начальства. Тем не менее случись такая ситуация, руководитель постарается установить ее причины, и если будет доказана вина администратора сети, и без того скромное вознаграждение станет еще меньше. Но творчески и заинтересованно подходя к своей работе, вы не будете испытывать дискомфорта и ощущения "давления сверху". Сеть должна работать не потому, что этого требует руководство, а потому, что это СЕТЬ.

Для кого и о чем эта книга

Администратор локальной сети — не столько профессия или должность, сколько образ жизни, а его квалификация — это жизненный опыт, опыт коллег, работающих в сетях, число которых ежегодно растет. С ростом числа сетей увеличивается и армия сетевых администраторов. Кому-то повезет, он получит возможность обучиться на специализированных курсах Microsoft, другим придется приобретать знания из книг и своих ошибок. Опыт коллег, несмотря на множество сайтов и отдельных страниц в сети Интернет, содержащих полезную информацию, не всегда доступен. Делаются попытки создать центры информации для системных администраторов и просто пользователей Windows 2000 и Windows 2003. Один из таких центров, который можно найти по адресу **http://www.rwntug.org.ru** — "Российская Группа

Пользователей Windows NT". Конференции и специализированные сайты в Интернете, а также целый ряд книг содержат массу информации по вопросам, связанным с работой системных администраторов. Тем не менее, информация эта либо отрывочна, либо подана на уровне, доступном профессионалам и специалистам с достаточно глубокими знаниями теории вопроса, либо изложена в энциклопедическом виде, и добраться до сути проблемы можно, лишь перелистав почти всю книгу, переходя от одной статьи к другой. Но на поиск решения иногда отведено весьма ограниченное время.

В этой книге вы почти не встретите теоретических сведений в основном тексте, она содержит практические примеры реализации различных задач администратора локальной сети, в большинстве своем предназначенные для работы в сети с сервером Windows 2000 Server или Windows Server 2003. Хотя примеры несложные, предполагается, что начинающий системный администратор, для которого предназначена книга, это все же не начинающий пользователь ПК. Для реализации примеров может потребоваться создание сценариев на языке VBScript, JScript или несложных программ на языке Visual Basic, который маститыми программистами порой не признается за полноценный язык программирования, но позволяет быстро создавать приложения, хорошо сопрягающиеся с продуктами Microsoft, а среда доступна и понятна для пользователей ПК с небольшим стажем. Описание языков программирования в книге не приводится, но если вы уже знакомы с основами программирования в среде Visual Basic, подробность описания примеров достаточна для повторения их на практике. На основе приведенных примеров вы сможете создать свой арсенал стандартных средств для работы в вашей сети, который поможет выполнять рутинные и достаточно трудоемкие часто встречающиеся задачи без значительных затрат времени. Невозможно описать в книге выполнение задач, подходящих для всех случаев жизни, но творческий подход к коллекции приведенных примеров позволит на их основе разработать свои собственные средства для решения именно ваших проблем. К созданию нового инструмента можно прийти, комбинируя старые, уже известные средства или составляющие этих средств. Большая часть примеров дана в виде описания уже сделанных настроек и не содержит излишне подробных инструкций типа "щелкните на кнопке (**кнопка 1**) в открывшемся окне (**окно 1**), выберите пункт меню такой-то" или — "начните работу с щелчка на кнопке **Пуск**". По мнению автора, такое подробное описание затрудняет проведение настроек и их понимание, а не облегчает их. Описания приводятся с иллюстрациями, по которым опытный пользователь ПК без труда их повторит.

В книге также даны описания некоторых полезных для работы администратора сети программ и утилит. Задачи по администрированию сети бывают настолько неожиданными, что для их решения в арсенале начинающего администратора не находится средств.

Существенное значение для успешной работы сетевого администратора имеет правильная организация своего рабочего места и "серверной". Некоторое внимание этому вопросу уделено в данной книге. Но эта информация не претендует на полноту и даже не носит рекомендательного характера, поскольку "на вкус и цвет товарищей нет", в каждой конкретной сети свои особенности организации работы администратора, а у каждого администратора могут быть свои предпочтения и материальные возможности. Но если у вас еще не сложилось представление о правильной организации своей работы и рабочего места, то эта информация может быть очень полезной на этапе организации работы системного администратора.

Кто-то из более опытных администраторов, прочитав эту книгу, может сказать, что в ней нет ничего нового. Да, это так. Вспомните слова Екклесиаста: "Что было, то и будет; и что делалось, то и будет делаться, нет ничего нового под солнцем. Бывает НЕЧТО, о чем говорят: “смотри, вот ЭТО новое”; но ЭТО было уже в веках, бывших до нас". Тем не менее, системным администраторам зачастую приходится либо "изобретать велосипед", либо "идти пешком", пробираясь сквозь тернии сетевых проблем, несмотря на то, что они уже были решены другими. Эта книга — опыт работы одного из администраторов, пытающегося решить проблемы сети с минимальными затратами, а не научный труд, в котором можно найти описание открытий и изобретений. Этим занимаются ученые и разработчики, результаты деятельности которых и применяются пользователями ПК, а также системными администраторами.

Рассмотренные примеры — это результаты экспериментов, поиска и кропотливого отбора существующих средств, которые не всегда бесплатны. Попытка применить лишь бесплатные программные продукты не привела к успеху. Если же вы легальный пользователь операционных систем Windows, то затраты на используемое коммерческое программное обеспечение не покажутся вам чрезмерными. Возможно, что к моменту выхода данной книги появятся и свободно распространяемые продукты, аналогичные описанным коммерческим, или вы найдете другие средства, более подходящие к вашим условиям. Во всяком случае, творчески подходя к своей работе, администратор должен постоянно быть в курсе новых решений и разработок, касающихся функционирования сетей.

Надеюсь, что время, потраченное на чтение этой книги и изучение примеров, не будет потеряно напрасно, и предложенная книга окажется полезным пособием при выполнении ваших ежедневных задач, связанных с поддержанием надежности и работоспособности сети, ее развитием и совершенствованием, особенно в начале вашей работы.

Если сведений, содержащихся в книге, окажется недостаточно или возникнут вопросы, связанные с выполнением конкретных задач, вы можете посетить

персональную страницу автора по адресу **www.okobox.narod.ru**. Там можно задать волнующие вас вопросы, обсудить возникшие проблемы, причем не только с автором, но и коллективно. Там же вы найдете и реализацию некоторых примеров, которые можно скопировать и с минимальными изменениями использовать в своей практике.

Для максимально комфортной работы с книгой следует ознакомиться с применяемыми сокращениями и обозначениями, помещенными далее, позволяющими более концентрированно изложить материал примера, не отвлекаясь на разъяснение сути примера в его пространном описании.

Принятые сокращения и обозначения

Для обеспечения компактности описаний примеров в книге применены сокращенные инструкции по работе с объектами операционной системы, которые можно увидеть в различных ее окнах. Под объектами будем понимать значки файлов, ярлыки программ, значки служб и свойств объектов, словом — любые значки, которые вы увидите в открытых окнах операционной системы и на рабочем столе. Применены также аббревиатуры для обозначения часто встречающихся наименований. Несмотря на кажущуюся вначале сложность запоминания приведенных ниже сокращений и обозначений, вы очень скоро привыкнете к ним и будете использовать в своей практике постоянно.

Аббревиатуры и сокращения

1. AD (Active Directory) — служба каталогов в Microsoft Windows 2000 и Microsoft Windows 2003.
2. DNS (Domain Name Services) — служба имен Интернета, применяемая также в системах Microsoft Windows 2000 и Microsoft Windows 2003. Для работы службы выделяются специальные серверы.
3. DHCP (Dynamic Host Configuration Protocol) — это протокол TCP/IP, автоматизирующий присвоение IP-адресов компьютерам (хостам), а также соответствующая служба. Для работы службы выделяются специальные серверы.
4. ИБП — источник бесперебойного питания.
5. ЛВС — локальная вычислительная сеть.
6. MUI (Multilingual User Interface) — многоязычный интерфейс пользователя.
7. ОС — операционная система.

8. Сервер — в зависимости от контекста, это главный компьютер сети, т. е. компьютер, на котором выполняется служба, обеспечивающая определенную функциональность в сети, или сама служба, работающая на сервере. Например, "Сервер DHCP" или "DHCP-сервер" — это или компьютер, на котором запущена соответствующая служба, или сама эта служба, когда разговор идет о конкретном компьютере-сервере. "Главный сервер" — компьютер, выполняющий функции основного сервера сети.

Выполнение операций с объектами ОС

1. Найдите **<Имя Объекта>** или Выделите **<Имя Объекта>** — это значит, что следует в уже открытом окне найти значок упоминаемого объекта и выделить его. В зависимости от индивидуальных настроек интерфейса, выделение может быть выполнено одинарным щелчком мыши на объекте или просто наведением указателя мыши на него.
2. Выберите **<Пункт Меню>** — это значит, что следует выбрать пункт меню, которое уже открыто перед вами, или щелкнуть правой кнопкой мыши на объекте и выбрать в контекстном меню **<Пункт Меню>** щелчком левой кнопки мыши. Некоторые команды могут быть вызваны двойным или одинарным щелчком мыши на объекте (в зависимости от индивидуальных настроек интерфейса), при этом команды, вызываемые по умолчанию, могут отличаться (в зависимости от индивидуальных настроек интерфейса). В связи с этим мы не будем применять двойной или одинарный щелчок мыши, кроме особо оговоренных случаев.
3. Выполните <Имя Команды> — это значит, что следует нажать кнопку **Пуск**, выбрать команду **Выполнить...**, набрать в поле ввода команды <Имя Команды> и нажать кнопку **OK**.
4. Разверните **<Имя Объекта>** — в ряде случаев около некоторых объектов вы увидите значок "+". Это значит, что внутри данного объекта содержатся другие, подчиненные ему объекты. Щелчком мыши (иногда двойным) на значке "+" этот объект можно развернуть, увидев дерево подчиненных ему объектов. Именно это действие и потребуется выполнить, когда вы увидите данную рекомендацию.
5. Откройте **<Путь>** | **<Имя Объекта>** — это значит, что следует выбрать пункт меню **<Открыть>** (см. п. 2) и тем самым открыть окно программы или службы, находящееся по одному из следующих адресов:
   - **Панель Управления** — Пуск | Настройка | Панель управления;
   - **Сетевые подключения** — Пуск | Настройка | Панель управления | Сетевые подключения;

- **Администрирование** — Пуск | Настройка | Панель управления | Администрирование;
- **IIS** — Пуск | Настройка | Панель управления | Администрирование | Службы Интернета;
- **Локальная Политика Безопасности** — Пуск | Настройка | Панель управления | Администрирование | Локальная политика безопасности;
- **Службы** — Пуск | Настройка | Панель управления | Администрирование | Службы;
- **Просмотр Событий** — Пуск | Настройка | Панель управления | Администрирование | Просмотр событий;
- **Управление Компьютером** (Computer Management) — Пуск | Настройка | Панель управления | Администрирование | Управление компьютером;
- **Система** — Пуск | Настройка | Панель управления | Система;
- **Учетные записи пользователей** — Пуск | Настройка | Панель управления | Учетные записи пользователей.

Ко многим упоминаемым окнам существуют и другие пути, но ввиду того, что меню **Пуск**, а также **Главное меню** пользователи часто настраивают "под себя", указаны пути, которые останутся неизменными практически при любой перенастройке интерфейса.

Если появится необходимость открыть окно, имя которого отсутствует в приведенном списке, то перед именем этого окна будет указан путь или имя окна, содержащего одноименный объект. Например, для открытия окна **Свойства: Интернет**, которого нет в списке, может быть указано: Откройте окно **Панель Управления | Свойства обозревателя**. Для открытия окна, которое не имеет заготовленного сокращенного обозначения пути, будет указан полный путь к объекту, который требуется открыть.

В зависимости от версии ОС, установленных пакетов обновлений, вариантов локализации, а также от некоторых других причин, имена объектов и названия окон могут встречаться и на русском, и на английском языке. В приложении дается список соответствия русских и английских наименований, которые могут быть приведены в окнах и меню по-английски, несмотря на то, что ОС локализована. В книге обычно будет указан только один вариант наименования, который присутствует на компьютерах, применявшихся для подготовки примеров.

Благодарности

Я благодарю всех, кто содействовал написанию этой книги.

Спасибо руководству организации, в которой я в настоящее время работаю. Оно не препятствовало творческому процессу, не запрещало использовать принадлежащее ему оборудование для проведения в выходные дни экспериментов по настройке сетевых сервисов и установке программ, подходящих для использования в локальной сети.

Спасибо редакторам, проводившим кропотливую работу по корректировке текста, выявлению неизбежных ошибок и участвовавшим в оформлении книги.

Спасибо Евгению Рыбакову, чья неоценимая поддержка и консультации позволили появиться этой книге.

Большое спасибо моей жене, которая относилась с пониманием и терпела мое отсутствие дома по выходным дням, пока шла работа над книгой.

ГЛАВА 1

Материальное и программно-техническое обеспечение сети

Предварительные замечания и рекомендации

В данной главе почти не приводится конкретных примеров, касающихся администрирования сети, но даются общие рекомендации по организации работы администратора, применению программных и аппаратных средств, без которых работа сети и ее администрирование мало эффективны. Поэтому наберитесь терпения и прочтите эту главу. Все рекомендации основаны на практическом опыте администрирования сети. Предполагается, что читатель — достаточно опытный пользователь ПК, знаком с работой компьютера в сети и имеет основные представления о работе самой сети. В зависимости от предварительной подготовки, материал этой главы может восприниматься как очень простой или как достаточно сложный. Если требуется дополнительная информация, можно порекомендовать книги того же автора "Сеть своими руками" или "Сеть под Microsoft Windows", в которых доступно описаны основы устройства сети. Там же даны подробные рекомендации по установке операционных систем.

Сеть, на основе которой готовились примеры, приведенные в данной книге, состоит из нескольких десятков компьютеров и двух серверов. Даже если в настоящее время ваша сеть значительно меньше, следует уже теперь думать о ее расширении. То есть все изменения, которые вы делаете сейчас в сети, должны предусматривать возможность подобного расширения. Имея в виду такую перспективу развития сети, мы и будем подбирать соответствующие средства и методы работы администратора.

Невозможно построить дом, не имея для этого соответствующих материалов, инструментов и механизмов, транспортных средств, не располагая площад-

кой, подготовленной для строительства, не разработав соответствующий проект и план строительства. Если вы только строите свою сеть, то книга поможет избежать серьезных промахов в ее планировании. Для администратора сети, основа которой уже построена и необходимо лишь обслуживание, поддержание в исправном состоянии и, в отдельных случаях, некоторая модернизация, полезной информации будет не меньше. Рекомендации, приведенные в этой главе, будут полезны во всех случаях.

Что же конкретно необходимо иметь в своем распоряжении администратору сети?

Рабочее место администратора локальной сети

Несмотря на то, что сеть может охватывать значительную площадь и войти в нее (авторизоваться) можно с любого подключенного к ней компьютера, лучше, если ваше рабочее место будет по возможности ближе к основному серверу сети. Более того, размещение рабочего места в непосредственной близости к серверу избавит вас от излишней ходьбы, если необходимо срочно предпринять какие-либо меры. Как бы надежно ни было оборудование и программное обеспечение, ни для кого не секрет, что всегда возможно "зависание" системы или отдельной программы. В этом случае даже наличие специальных средств удаленного управления не позволит оперативно решить проблему. Необходимо личное присутствие администратора около сервера. При этом ваше рабочее место, точнее рабочий компьютер, не должен совпадать с компьютером-сервером. Несмотря на высокий уровень подготовки, никто не застрахован от ошибок. А ошибка, допущенная при работе на сервере, может стать причиной простоя сети в течение продолжительного времени. Конечно, полностью исключить необходимость выключения или перезагрузки сервера невозможно, но время проведения этих операций и их количество должно быть минимизировано.

Из своей практики могу сказать, что более или менее серьезные остановки сети (на 10—30 минут) требуются не чаще одного раза в сто дней, а короткие перерывы в работе сети, связанные с проведением обновления программного обеспечения, — не чаще одного раза в месяц, причем сам перерыв длится три-четыре минуты. Если учесть, что для выполнения таких процедур выбирается время, когда большая часть пользователей сети не работает, то у них складывается ощущение, будто сеть никогда не останавливается, а именно к этому и следует стремиться.

Таким образом, наиболее удобный вариант расположения рабочего места — это "серверная" (отдельное помещение, где расположен сервер или серверы).

Само собой разумеется, что от компьютеров сети, коммутаторов, расположенных в сети, от других сетей, возможно, взаимодействующих с вашей, к

серверной подходит значительное число кабелей. Часто начинающие администраторы считают, что когда возникнет необходимость, можно изменить подключения, переложить кабели, заменить оборудование. На самом деле, если заранее не предусмотреть возможности расширения сети, наступит момент, когда она будет неработоспособна продолжительное время, которое может составлять не один день; даже после восстановления ее работоспособности вам еще придется завершать начатые работы не одну неделю. Лучше заранее готовиться к будущим проблемам. Естественно, что такая подготовка потребует некоторых затрат, которые на данный момент "не требуются", но эти затраты необходимы. Если выделение средств на техническое обеспечение вашей сети зависит от руководства организации, в которой эксплуатируется сеть, постарайтесь доказать, что затраты необходимы именно теперь. Позднее затраты будут выше, учитывая потери, к которым приведет продолжительный простой сети, а также оплату за работу, которая будет выполняться. Приведем небольшой пример, который поможет и вам, и вашему руководству понять необходимость таких затрат. На рис. 1.1 показан ввод кабелей в серверную и их подключение к коммутирующим устройствам в наименее затратном (на момент проведения работ) варианте.

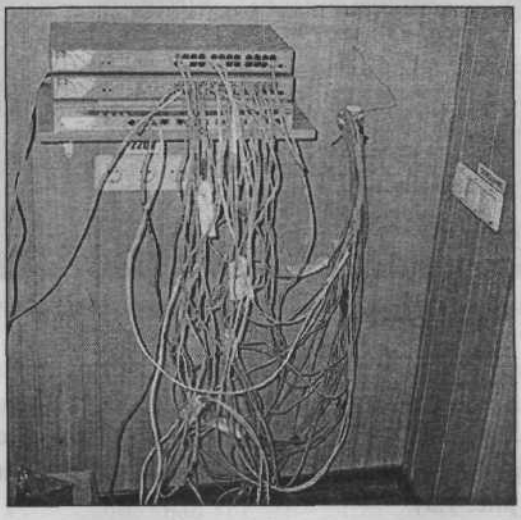

Рис. 1.1. Упрощенная коммутация кабелей и размещение оборудования

Представьте себе, что кто-либо задел случайно эту "бороду" из кабелей, споткнулся и потянул кабели за собой... Как ни удивительно, но именно такой вид организации физических подключений применяется во многих локальных сетях, особенно в тех, где администратор не имеет достаточного опыта. Предположим теперь, что потребовалось добавить еще десяток-другой подключений — результат очевиден.

В данном случае затраты были бы невелики, а работ по изменению подключения этих кабелей не пришлось бы выполнять, если бы сразу был применен другой вариант их организации при вводе в серверную. Такой вариант показан на рис. 1.2.

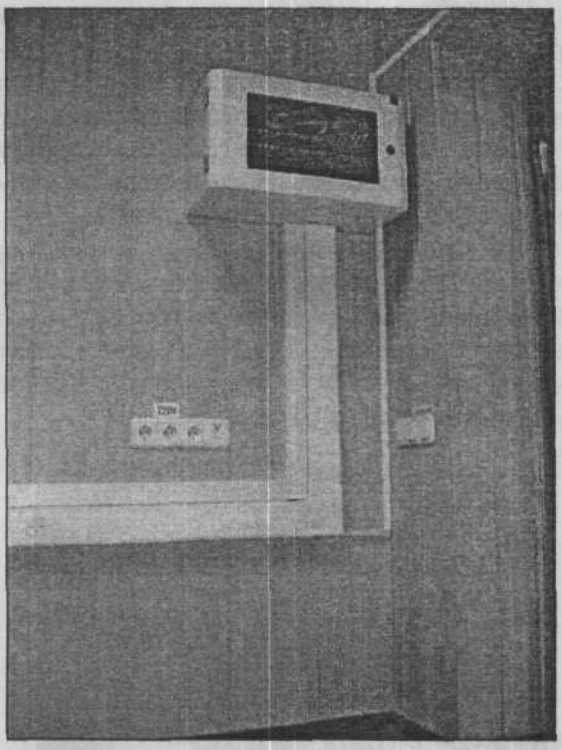

Рис. 1.2. Нормальная коммутация кабелей и размещение оборудования

Теперь нет некрасиво и опасно расположенных кабелей, они аккуратно скрыты в коробах, а их подключение осуществлено через специально для этого предназначенные коммутационные панели (патч-панели) с организаторами кабеля. Часть активного оборудования осталась здесь же в настенном коммутационном шкафу (рис. 1.3).

Немаловажно, что шкаф может быть закрыт на замок. При этом значительно уменьшается вероятность случайного доступа к кабелям и оборудованию, находящемуся в шкафу. Возле каждого гнезда на патч-панелях должны быть этикетки с подписями о назначении данного соединения. Неплохо иметь и список всех гнезд с указанием их назначения.

Конечно, самостоятельно вы вряд ли сможете установить такой шкаф. Для этого лучше пригласить специалистов, которых смогут вам порекомендовать

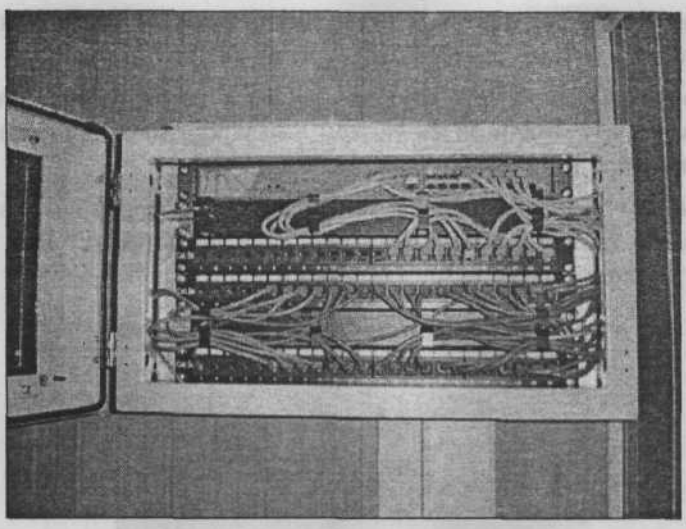

Рис. 1.3. Коммутационный шкаф с открытой дверцей

поставщики оборудования. Вместе с коммутационным шкафом потребуется приобретение кабельного канала — короба, в котором будут находиться кабели. Существуют различные конструкции кабельных каналов. Есть такие варианты их конструкции, которые предусматривают не только прокладку кабеля, но и размещение компьютерных розеток прямо на их корпусе. При этом к таким розеткам можно подключать не только компьютерный кабель, но и телефонный. Стандартный телефонный разъем меньше компьютерного (четыре или два контакта вместо восьми), но прекрасно включается в гнездо компьютерной розетки. На рис. 1.4 показаны включенные в одинаковые гнезда компьютерной розетки телефонный провод и коммутационный шнур (патч-корд), соединяющий с сетью компьютер.

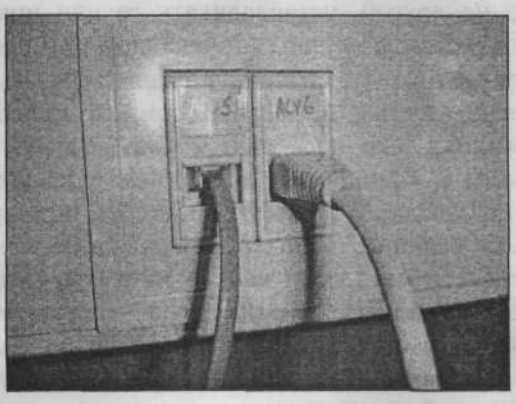

Рис. 1.4. Телефонный и компьютерный кабели подключены в одинаковые гнезда

Конечно, с внутренней стороны к этим гнездам должны подходить соответствующие кабели — один телефонный, другой компьютерный.

Если телефон или компьютер не подключены к такой розетке, то ее гнезда закрываются подпружиненной заслонкой, что исключает загрязнение и попадание в них посторонних предметов (рис. 1.5).

Мы не указываем здесь конкретные типы кабельных каналов и коммутационных шкафов, вы сможете выбрать те, что больше подойдут вам из предложенных торгующими подобными товарами организациями.

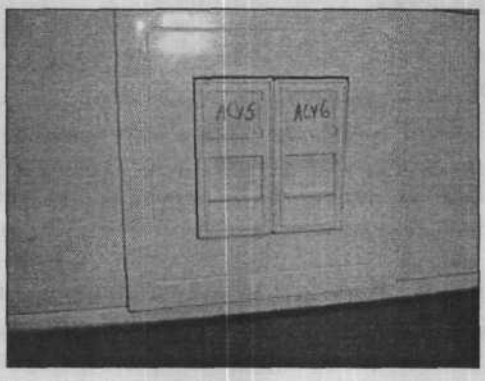

Рис. 1.5. Гнезда розеток, закрытые заслонками

Рабочий компьютер

Основной инструмент администратора — компьютер. Каким он должен быть? Несмотря на возможные материальные трудности, необходимо, чтобы этот компьютер был современным, желательно мобильным. Если это обычная рабочая станция, вам придется в ряде случаев переносить информацию с одного компьютера на другой, устанавливать те или иные программы на компьютеры, находящиеся в различных точках сети или вне ее. Согласитесь, что возможность контролировать ситуацию в вашей сети из любой географической точки совсем не лишняя, мобильный компьютер позволяет упростить процедуру подключения к сети, поскольку можно заранее установить все необходимые программы и выполнить соответствующие настройки. Если на данный момент вы не обладаете таким компьютером, постарайтесь включить его приобретение в ближайшие планы, убедите ваше руководство в необходимости этой покупки. Это позволит вам во многих случаях не выезжать к месту, где находится ваша сеть, для оперативного решения проблем, требующих вашего вмешательства. Можно иметь, конечно, настроенный соответствующим образом компьютер и дома, но тогда вы в определенной степени ограничите свободу работы на нем.

Конкретный тип компьютера указать сложно. Техника развивается, появляются новые модели компьютеров с новыми возможностями, но важно, чтобы ваш мобильный компьютер мог заменить обычную рабочую станцию, он должен иметь встроенный модем. Как ориентир, можно указать ноутбук Compaq nx9010 с 512 Мбайт оперативной памяти и жестким диском 30 Гбайт (именно такой компьютер применяется автором). На этих компьютерах обычно уже установлена операционная система Windows XP Pro, которую потребуется лишь настроить под ваши потребности. Подключение внешней клавиатуры и мыши повысит комфортность работы на вашем обычном рабочем месте.

Оборудование серверной

Кроме вашего рабочего компьютера, в серверной, являющейся вашим рабочим помещением, должен быть расположен и сам сервер (возможно, не один), модемы, коммутаторы, концентраторы (хабы), маршрутизаторы, источник бесперебойного питания (ИБП). В зависимости от размеров сети и ее назначения, не все перечисленные виды оборудования могут применяться в вашей сети в данный момент. Но без ИБП сервер подвержен риску быть выведенным из строя при случайных бросках напряжения питающей сети. Кроме того, возможны перебои в работе локальной сети при кратковременном отключении напряжения. Даже когда сервер подключен к отдельной линии "чистого" питания, остается риск отключения напряжения.

Если на данный момент перечень оборудования невелик и все оно помещается на одном столе, то обязательно придет время, когда этот перечень увеличится. Но даже имея скромный список применяемых устройств, на столе лучше поместить монитор, мышь и клавиатуру. Все остальные устройства следует разместить в специальной стойке — шкафу (рис. 1.6). Этим вы "убьете двух зайцев": во-первых, вы освободите пространство в серверной, а во-вторых, дадите возможность сети развиваться без лишних проблем для себя.

Именно в таком состоянии развития сейчас находится сеть, в которой применяется эта стойка. В нижней трети стойки можно рассмотреть свернутый петлей тонкий оптоволоконный кабель. В данный момент ожидается установка оптического модема, а два канала оптоволоконной линии соединены для проверки качества связи со стороны внешней сети. Как видите, промежуточные состояния комплекта оборудования никак не отражаются на интерьере серверной и не мешают работе. А прозрачная дверь шкафа-стойки защищает все оборудование от случайного воздействия посетителей серверной, но позволяет видеть индикаторы на оборудовании, которые несут важную информацию о состоянии сети.

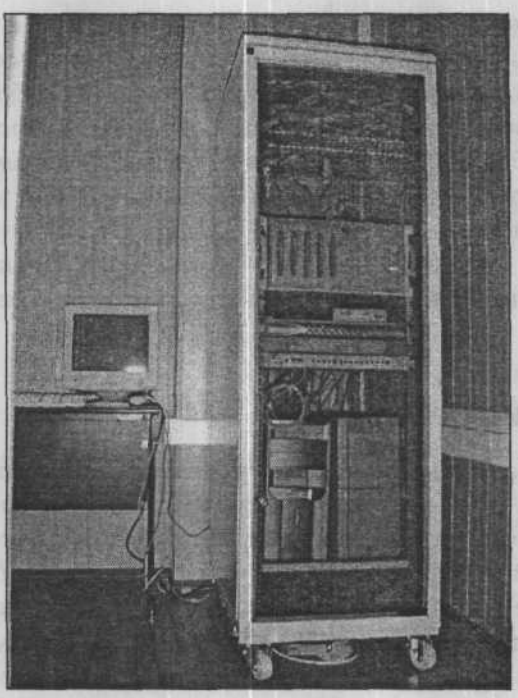

Рис. 1.6. Компьютерная стойка с оборудованием

Программное обеспечение

О программном обеспечении серверов сети мы будем говорить в следующих главах. А пока рассмотрим те программные продукты, которыми желательно запастись для успешной работы по администрированию вашей сети и для создания некоторых полезных инструментов администратора.

Сначала об операционной системе. Пожалуй, наиболее распространенной операционной системой на компьютерах пользователей стала Windows XP. ОС вашего компьютера должна быть не ниже чем Windows XP Professional. Это позволит выполнять все необходимые операции по обслуживанию сети, многие из которых недоступны для операционных систем более низкого уровня. Кроме того, ваша ОС должна содержать, по возможности, все последние обновления. Прежде всего, это касается обновлений критических, которые корпорация Microsoft настоятельно рекомендует устанавливать в первую очередь. Язык операционной системы может быть любым, но, учитывая, что обновления выходят в первую очередь для англоязычной версии системы, ее и следует применять, для удобства работы установив интерфейс пользователя на родном языке с помощью пакета MUI (Multilingual User Interface, многоязычный интерфейс пользователя). Для национальных версий

систем, в том числе и для русскоязычной, обновления выходят на несколько недель позднее. Теперь о дополнительных приложениях и утилитах. Список применяемых администратором программных продуктов может быть весьма широк. Одни будут применяться часто, другие вообще могут лежать и ждать случая для своего использования. Например, средства для восстановления информации с "упавшего" сервера могут не пригодиться никогда, но иметь их в своем арсенале необходимо. Конкретные программы в основном будут рассматриваться по ходу изложения и по мере необходимости. Сейчас отметим лишь основные виды приложений, которые желательно иметь на вашей рабочей машине.

1. Основные офисные приложения, такие как MS Word, MS Excel, MS Access.
2. Текстовый редактор, позволяющий редактировать документы в различных кодировках. Таких редакторов может быть несколько, поскольку применение того или иного из них наиболее удобно в каждой конкретной ситуации.
3. Редактор Web-страниц. Можно для этой цели применять и обычный текстовый редактор "Блокнот", входящий в состав операционной системы, но часто удобнее применять специализированную программу.
4. Файловый менеджер. Несмотря на развитые возможности операционной системы, очень полезен файловый менеджер FAR, разработанный специально для ОС Windows и прекрасно работающий во всех ее версиях. Дополнения (plugins), в изобилии имеющиеся для этого файлового менеджера, позволяют эффективно использовать его для решения самых различных задач при работе с файлами в сети.
5. Потребуются некоторые специализированные программы, такие как сканеры сети. С их помощью вы всегда сможете определить доступность компьютера в сети, определить доступные порты, решить другие задачи, связанные с обслуживанием сети.
6. Несмотря на то, что в офисных приложениях от Microsoft имеются встроенные средства для работы с языком программирования Visual Basic for Application, желательно установить среду разработки программ на языке Visual Basic. Автор применяет Visual Basic 6, который можно найти как в составе Visual Studio, так и отдельно.
7. Средства удаленного администрирования. В книге будет рассмотрено применение программы Radmin, которая разработана в России, но возможно применение и других разработок.
8. В ряде случаев потребуются простой почтовый сервер, Web-сервер. Причем Web-сервер должен быть реализован в применяемой операционной системе (Windows XP, Windows 2000 Server или Windows Server 2003), а

в качестве почтового сервера может быть использован встроенный в Windows Server 2003 или потребуется программа сторонних разработчиков.

9. Почтовый клиент. Обычный почтовый клиент, скорее всего, вами давно применяется, но понадобится также консольный почтовый клиент, наличие которого позволит автоматизировать целый ряд задач, связанных с администрированием сети.
10. В качестве дополнительного программного обеспечения неплохо иметь программный эмулятор компьютера. С его помощью можно создать виртуальный компьютер прямо на вашей рабочей станции и проводить целый ряд экспериментов, безопасных для вашей сети. После удачного завершения экспериментов с новыми программными инструментами можно будет применить их в сети, не опасаясь, что ошибки приведут к непоправимым последствиям.
11. Антивирусный пакет. Применение такого программного обеспечения обязательно.
12. Консольный архиватор PKZip. Этот архиватор, работающий в командной строке, необходим для автоматизированного выполнения некоторых задач. Windows XP имеет встроенные средства для создания и распаковки ZIP-архивов, но дополнительно может понадобиться архиватор RAR, ввиду широкого распространения архивов данного формата.
13. Инструменты администратора, входящие в состав ОС. Они обязательно имеются в профессиональной версии операционной системы. Некоторые дополнительные средства находятся на инсталляционном диске Windows XP, и устанавливать их следует отдельно (поскольку они не устанавливаются в ходе инсталляции системы).

Список получился достаточно внушительным, но значительная его часть уже есть в вашем распоряжении, а то, чего нет, будем устанавливать по мере необходимости.

О политике распределения сетевых адресов

Основная группа сетевых протоколов, применяемых при построении локальных сетей, это IP-протоколы, первоначально созданные для организации сети Интернет, что и сохранилось в их названии — Internet Protocols. Развитие сетевых технологий привело к повсеместному применению этих протоколов при организации сетей любого масштаба. Протоколы, применявшиеся в локальных сетях до распространения IP-технологий, теперь почти не встречаются в них. Исключение могут составлять очень маленькие одноранговые

сети, которые в данной книге не рассматриваются, или сети специального назначения. Само собой, и в вашей сети применяются IP-протоколы. Для успешного распознавания и идентификации компьютеров в сети каждый компьютер обязан иметь уникальный IP-адрес.

Уникальность IP-адреса является одной из основ бесперебойной работы сети. Тем не менее количество IP-адресов не безгранично. Это касается как сети Интернет, так и локальной сети. Для обеспечения каждого работающего в сети компьютера уникальным адресом применяется динамическое присвоение адреса при входе в сеть. Эта технология позволяет обеспечить уникальным адресом значительно большее число компьютеров, чем их может одновременно работать в сети, если периоды их работы не совпадают. В локальной сети обычно рассчитывают на то, что все компьютеры сети могут работать одновременно. В связи с этим выгода от применения динамического способа выделения сетевых адресов несколько уменьшается. Но одно его преимущество остается. Администратору не требуется следить за уникальностью адреса каждого компьютера сети. За него это делает серверная операционная система. К сожалению, этот способ выделения IP-адресов применим не всегда. Не вдаваясь в подробности, можно сказать, что его применение устанавливает некоторые ограничения для рабочих станций сети. Поэтому нам придется вести "двойную бухгалтерию" — часть адресов будет выдаваться динамически, другие же (в том числе и ваш при работе в сети) должны быть статическими. За уникальностью этих адресов придется следить вам. Для того чтобы не запутаться в этой "бухгалтерии", важно с самого начала определить для себя правила, которым должно подчиняться распределение IP-адресов вашей сети. Если до настоящего времени это не сделано и количество компьютеров сети невелико, не поленитесь определиться с этими правилами и выполнить необходимые операции для их соблюдения.

Прежде всего следует уделить внимание выбору IP-адреса самой сети. По умолчанию на серверах Windows 2000 Server и Windows Server 2003 для ЛВС предлагается адрес 192.168.0.0 с маской подсети 255.255.255.0. Соответственно для сервера предлагается адрес 192.168.0.1. Для самых простых замкнутых на себе сетей это хороший выбор. Но если рассчитывать на расширение сети и взаимодействие с другими локальными сетями (применяя, например, маршрутизаторы), то этот выбор приведет в дальнейшем к проблемам, которые можно решить лишь достаточно трудоемким способом. В качестве примера такой проблемы можно привести следующую ситуацию.

Допустим, требуется подключиться к другой локальной сети. Сервер этой локальной сети имеет адрес 192.168.0.20. Ваш DNS-сервер содержит запись с таким адресом для одной из рабочих станций. Соответственно, DHCP-сервер вашей сети выдал этот адрес рабочей станции и следит за его уникальностью,

но тут требуется найти компьютер в другой сети с адресом, который соответствует одному из адресов вашей ЛВС. Попытка подключения к такому серверу обречена на неудачу. Ваш сервер не разрешит это подключение. Ни с одного компьютера вашей сети вы не сможете обнаружить такой внешний сервер. Конечно, существуют пути решения и такой проблемы, но они достаточно трудоемки. Все решается значительно проще, если сети имеют различные адреса. Необходимость смены адреса сети может привести даже к конфликту между администраторами — в какой из двух сетей следует менять адрес? Если же вы сразу, пока сеть не велика, или даже на стадии ее первоначальной настройки выберите иной адрес, то вероятность конфликта резко снизится. Какой же адрес следует выбрать? Ответ может быть подсказан наименованием вашего предприятия (они часто содержат номера), адресом здания, где организована сеть, или другими ассоциациями. Найденное "свое" число можно поместить в третьем блоке адреса. Предположим, что это число — 115. Адрес вашей сети в этом случае может выглядеть так: 192.168.115.0. Первые две тройки чисел лучше не изменять. Причина этого запрета заключается в том, что все возможные адреса распределены по областям их применения. Одни для небольших локальных сетей, другие — для Интернета, третьи — для крупных сетей, но еще не глобальных, четвертые для экспериментальных сетей, и т. д. Если какая-нибудь сеть присвоит себе адрес, который должен принадлежать другой группе сетей... ничего страшного не произойдет. Но возможны проблемы при контактах с другими сетями. Лучше, соблюдая принятые правила, присвоить сети адрес 192.168.115.0. Если происходит организованное создание нескольких сетей, между которыми предполагается взаимодействие, то следует сразу договориться о распределении IP-адресов. Обезопасив себя таким образом от возможных внешних проблем, можно приступить к внутреннему распределению адресов.

Необходимо определиться также с диапазонами адресов, которые вы будете применять для различных целей. Работоспособность сети не зависит от того, как будут распределены адреса, если все они допустимы для этой сети. Но, как и в любой системе, сетью управлять проще, когда она организована по правилам. Вариант, который можно предложить для разбиения всего доступного в сети адресного пространства на диапазоны, показан в табл. 1.1.

При таком разбиении адресов на диапазоны в вашей сети "есть место" для 170 компьютеров. Сорок девять из них могут иметь фиксированные адреса, а сто двадцать один могут получать адреса автоматически. Скорее всего, такого количества рабочих станций (серверы не входят в это число) в нашей сети пока нет, и свободных адресов достаточно для дальнейшего ее развития. При необходимости вы можете несколько изменить предложенный порядок распределения адресов. Но если конкретных планов развития сети еще нет, то лучше применить такой.

Таблица 1.1. *Диапазоны адресного пространства в сети*

Символ	Диапазон адресов	Число устройств	Назначение диапазона
B (begin)	192.168.115.0	0	Не применяется для устройств сети
S (servers)	192.168.115.1–192.168.115.15	15	Адреса существующих и предполагаемых серверов
P (printers)	192.168.115.16—192.168.115.25	9	Адреса существующих и предполагаемых принт-серверов
R (routers)	192.168.115.26—192.168.115.50	25	Адреса существующих и предполагаемых устройств, связанных с межсетевым взаимодействием (маршрутизаторов, например)
F (fixed)	192.168.115.51—192.168.115.99	49	Адреса компьютеров вашей сети с фиксированными IP-адресами
D (dynamic)	192.168.115.100—192.168.115.220	121	Адреса компьютеров вашей сети с адресами, назначаемыми сервером DHCP
X (x)	192.168.115.221—192.168.115.244	24	Зарезервированный диапазон адресов
E (end)	192.168.115.255	0	Не применяется для устройств сети

О главном сервере

В качестве такового лучше применить компьютер под управлением ОС Windows Server 2000. Хорошо, если этот компьютер имеет именно серверную конфигурацию. В этом случае его надежность существенно выше, чем у обычного компьютера. Проконсультироваться относительно лучшего варианта конфигурации вы можете у продавца компьютерной техники. В качестве ориентира для поиска наиболее подходящей конфигурации можно указать на следующие особенности сервера. Лучше, если это двухпроцессорная машина с жесткими дисками (не менее двух), которые можно использовать для работы в дисковом массиве. Это один из способов повышения надежности серве-

ра. Или диски должны работать в режиме отражения, когда для повышения надежности хранения информации она записывается на оба диска. В случае возникновения проблем с одним из винчестеров, сервер может продолжать работу, а после восстановления неисправного устройства его диски снова будут работать в режиме дублирования записи. Для пользователя, работающего с таким сервером, в системе будет виден лишь один диск. Распространен режим работы в массиве RAID (Redundant Array of Independent Disks, избыточный массив недорогих дисков). Есть несколько вариантов реализации данного режима. На странице **http://www.ixbt.com/storage/raids.html** приведена подробная статья, описывающая все варианты реализации режимов работы дисков в массиве. Настройку таких режимов работы лучше доверить специалистам организации, где вы будете приобретать сервер. Если высокой надежности от вашего сервера не требуется, то можно обойтись и обычным режимом работы дисковой системы, установив единственный винчестер.

Установка ОС на сервер до начала его настройки в качестве сервера ничем не отличается от обычной установки операционной системы. Далее запускается мастер настройки сервера, ответив на вопросы которого вы завершите первичную его настройку. Вы можете доверить эту процедуру специалисту, порекомендованному продавцом компьютера. Но подробности конфигурации сервера, ее нюансы рекомендуется выполнять самостоятельно.

Следует обратить внимание на то, что при первоначальной настройке сервера необходимо правильно указать его роль в сети. Не "упрощайте" себе жизнь, — не создавайте сеть с рабочей группой (или группами). Чтобы эффективно управлять сетью и иметь возможность дальнейшего ее развития, сразу создайте домен (область сети), а сервер должен стать контроллером домена. Имя домена может быть любым, но подчиняющимся правилам создания доменных имен. Правила совсем несложные. Имя вашего домена должно состоять из двух частей, разделенных точкой, и быть написано латинскими строчными буквами. Левая часть — это собственно и есть имя вашего домена, а правая — имя домена верхнего уровня. Если бы мы создавали наш домен как часть Интернета, следовало бы указать имя зоны, в которой зарегистрирован наш домен. Но наша сеть самостоятельная, домен не зарегистрирован, поэтому в левой части можно указать вымышленное имя зоны, например "dom". Полное имя нашего домена будет выглядеть так: mydomain.dom. Вы можете выбрать любое имя зоны, но оно не должно совпадать с именами известных зарегистрированных зон (ru, com, ua, mil, da, org и др.). Совпадение с именами зон в других сетях вполне допустимо, но имена доменов должны отличаться.

После того как основные настройки сервера выполнены, необходимо установить службу каталогов Active Directory. Установка этой службы приведет к запрещению создания локальных пользователей компьютера-сервера. Только

администратор компьютера, пароль которого был назначен в процессе установки системы, будет иметь возможность входить в систему локально со всеми привилегиями. Далее можно создать любое число пользователей с правами администратора, если это необходимо, или вообще без прав, но учетные записи будут создаваться в рамках домена. При этом, если не указать в правах новых пользователей возможность локального входа в систему, они этого сделать не смогут, все их права будут применяться для работы в сети, когда они будут авторизоваться в ней со своей рабочей станции. Компьютеры пользователей могут настраиваться в такой сети и как члены рабочей группы, и как члены домена. Каждый вариант настройки имеет свои особенности, о которых будет рассказано в соответствующих примерах. Первоначальная настройка службы каталогов производится автоматически с помощью мастера настройки сервера. Если ваш сервер еще не работает, и вы только намерены инсталлировать его, но не уверены, что у вас все получится, то доверьте эту процедуру специалистам или предварительно прочтите другую литературу на эту тему. Можно рекомендовать книгу этого же автора "Сеть под Microsoft Windows", вышедшую в издательстве "БХВ-Петербург" в 2003 г. В общем случае, для больших сетей служба каталогов представляется довольно сложной структурой, о которой вы можете прочитать в справочной системе Windows. В нашей сети эта служба будет представлена в самом простом своем варианте, поскольку будет содержать лишь один контроллер домена и одна подсеть. К интерфейсам AD мы будем обращаться в процессе рассмотрения примеров администрирования в других главах книги. Если ваш сервер только что установлен, то отсутствие настроек в AD приведет лишь к тому, что будет всего один зарегистрированный пользователь сети — ее администратор. В следующих главах будут предложены примеры, связанные с управлением службой каталогов.

Сейчас рассмотрим только пример настройки DHCP-сервера для обеспечения возможности применения предложенных диапазонов IP-адресов. DHCP-сервер лучше располагать на основном сервере вашей сети. Технически возможны и другие варианты его расположения, но в небольшой сети нет смысла приобретать для этого отдельный сервер. При описании этого примера исходим из предположения, что на вашем сервере уже установлена операционная система Windows 2000 Server (русская версия), а также серверы DNS, DHCP, WINS.

Настройка сервера DHCP

В данном примере показан уже настроенный для конкретной сети сервер DHCP. Имя основного сервера в вашей сети иное. Могут отличаться и другие описываемые параметры и настройки. Если необходимо изменить что-либо в настройках сервера, — изменяйте, но обязательно ведите записи обо всех

вносимых изменениях, чтобы можно было вернуться к исходному состоянию сервера в случае ошибки.

Итак...

Откройте **Администрирование | DHSP**.

Вы увидите окно **DHCP** (рис. 1.7), в левой части которого находится значок вашего сервера с указанием IP-адреса. Разверните объект <Имя вашего сервера>, вы увидите папку **Область** и значок параметров сервера. Часть необходимых параметров и объектов этого окна была установлена при инсталляции сервера. Но теперь нам необходимо настроить распределение адресов в соответствии с выбранной политикой. Для этого разверните папку **Область** и найдите **Пул адресов** (рис. 1.8). В правой части окна отобразится диапазон адресов для аренды. Адреса из этого диапазона будут выдаваться сервером DHCP рабочим станциям. Для изменения этого диапазона снова найдите **Область** и в меню **Действие** окна **DHCP** выберите пункт **Свойства**.

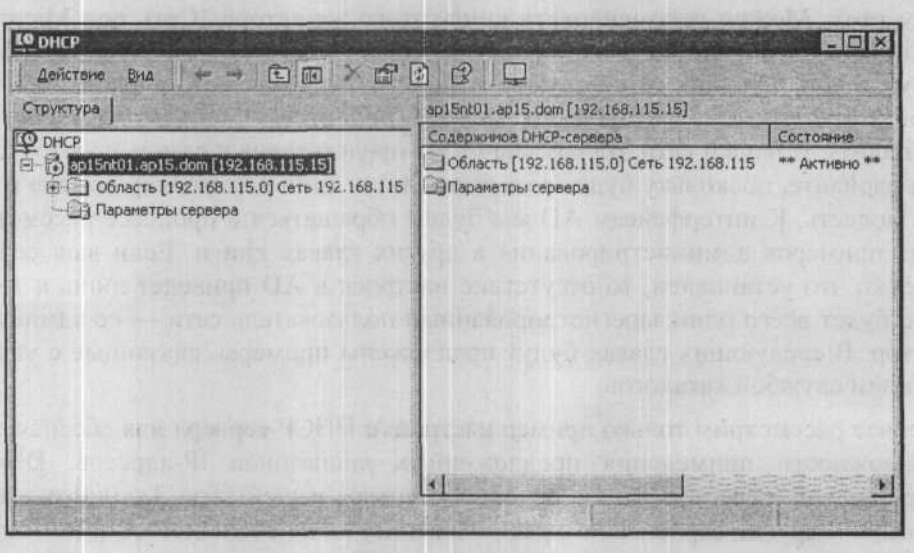

Рис. 1.7. Окно DHCP

Примечание

Надо сказать, что содержание меню **Действие** зависит от того, какой объект в окне выделен.

Перед вами откроется окно **Свойства: Область** (рис. 1.9). В этом окне вы можете изменить имя области, ее начальный и конечный адрес, а также срок аренды адреса. Срок аренды определяет время, в течение которого этот адрес будет "закреплен" за рабочей станцией, если она длительное время не входит в сеть. Начальный и конечный адрес области может быть ограничен не толь-

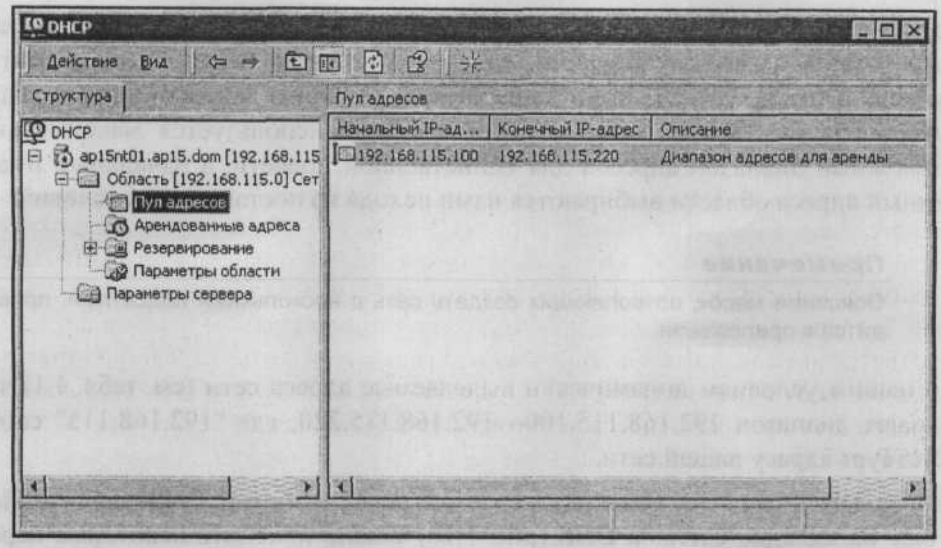

Рис. 1.8. Окно **DHCP** (развернута папка **Область**)

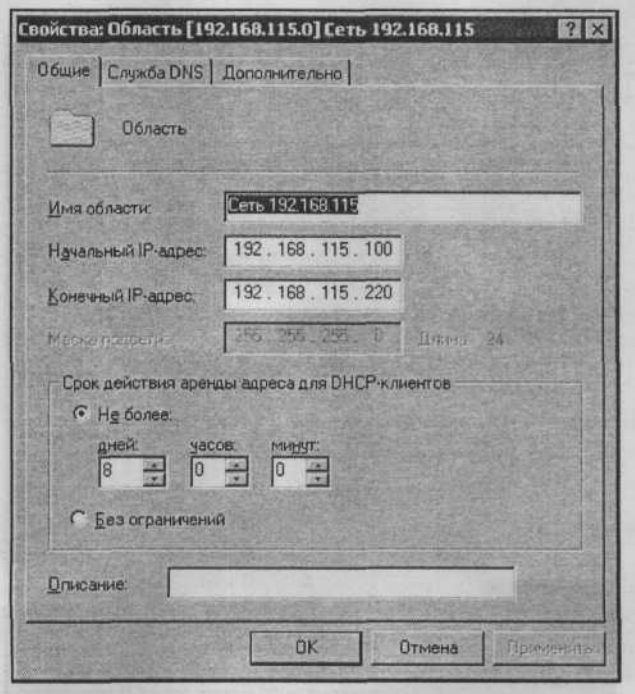

Рис. 1.9. Окно **Свойства: Область** (вкладка **Общие**)

ко нашим выбором, но и свойствами самой области. Если, например, вы хотите создать несколько подсетей, каждая из которых имеет маску подсети, отличную от 255.255.255.0, то начальный и конечный адреса будут определяться соответственно маске. В нашем случае используется максимально возможный диапазон адресов для единственной подсети, а начальный и конечный адреса области выбираются нами исходя из поставленных условий.

Примечание

Описание масок, позволяющих создать сеть с несколькими подсетями, приводится в приложении.

По нашим условиям динамически выделяемые адреса сети (см. табл. 1.1) занимают диапазон 192.168.115.100—192.168.115.220, где "192.168.115" соответствует адресу вашей сети.

Работа DHCP-сервера довольно тесно связана с работой DNS-сервера. Поэтому на вкладке **Служба DNS** (рис. 1.10) можно изменить некоторые параметры работы сервера. Если вы не замечали неполадок в работе сервера, то лучше оставить настройки такими, как на рис. 1.10.

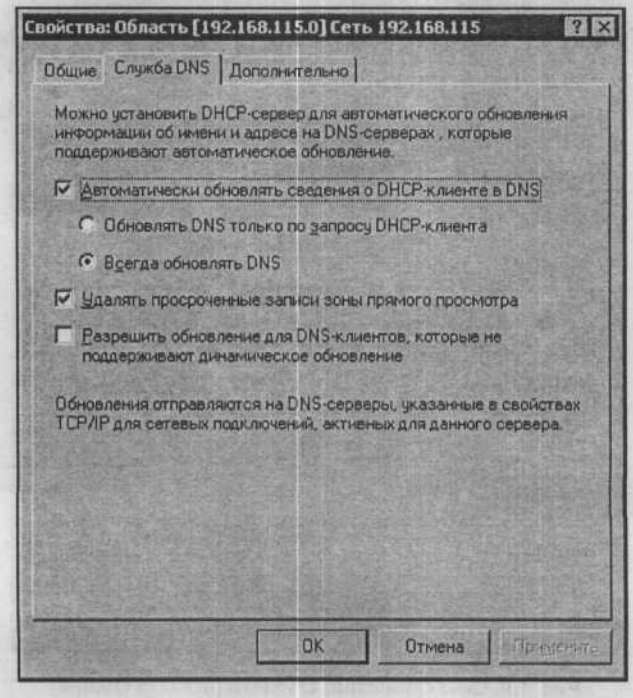

Рис. 1.10. Окно **Свойства: Область** (вкладка **Служба DNS**)

После установки и настройки DHCP-сервер начинает выдавать адреса компьютерам сети при условии, что в настройках TCP/IP каждой рабочей станции указано: **Получить IP-адрес автоматически**. Уже выданные адреса можно увидеть в окне **DHCP**. Для этого выделите пункт **Арендованные адреса** в развернутом дереве области и посмотрите на правую часть окна. Там вы увидите подробную информацию о том, кому, какой адрес и до какого времени выдан.

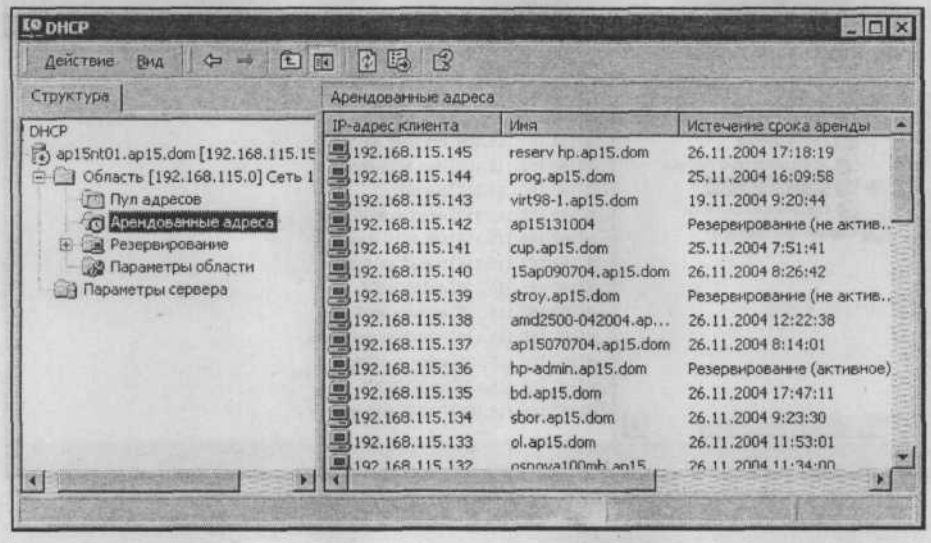

Рис. 1.11. Окно **DHCP** (**Арендованные адреса**)

Если сервер DHCP уже работал в вашей сети, и вы решили только изменить диапазон выдаваемых адресов, то прежде чем проводить настройку, посмотрите на арендованные адреса. Если некоторые из них выходят за пределы выбранного нами диапазона, то вы можете пойти двумя путями:

- Сместить диапазон выдаваемых сервером адресов в сторону уже выданных. При этом следует внести коррективы в табл. 1.1.
- Дождаться момента, когда рабочие станции с адресами, выходящими за пределы диапазона "D", завершат работу, и удалить их из числа арендованных. После установки начального и конечного адреса диапазона сервер снова выдаст адреса рабочим станциям при первом их входе в сеть, но уже из установленного диапазона.

В правой части окна (рис. 1.11) вы можете увидеть, что в графе **Истечение срока аренды** для некоторых рабочих станций стоит значение "Резервирование" (активное или не активное). Такое резервирование вы можете создать, если необходимо, чтобы рабочая станция пользовалась услугами сервера

DHCP, но ее адрес не изменялся даже при длительном отключении этой рабочей станции от сети. Иными словами, срок аренды адреса для этих рабочих станций устанавливался неограниченным. Для просмотра уже зарезервированных адресов выделите пункт **Резервирование** в левой части окна (рис. 1.12) и посмотрите список адресов в правой части окна.

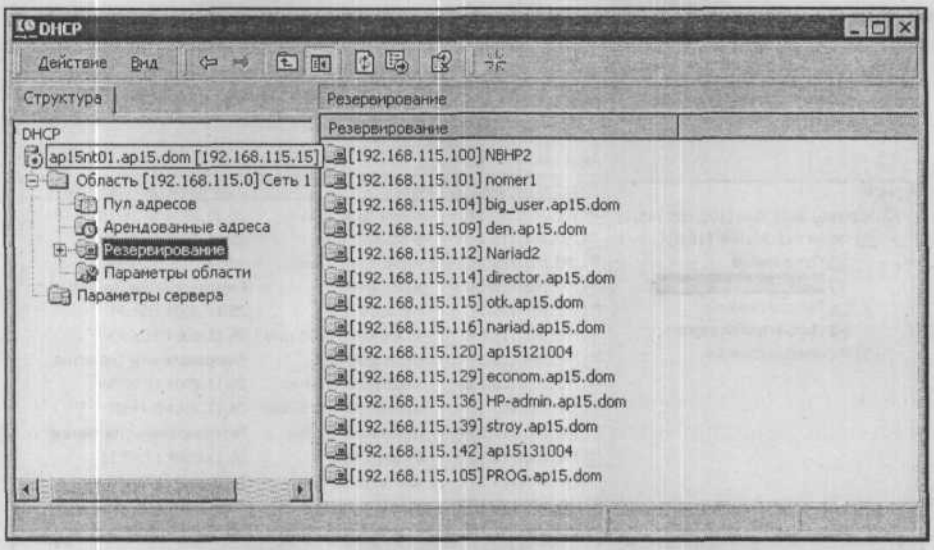

Рис. 1.12. Окно **DHCP (Резервирование)**

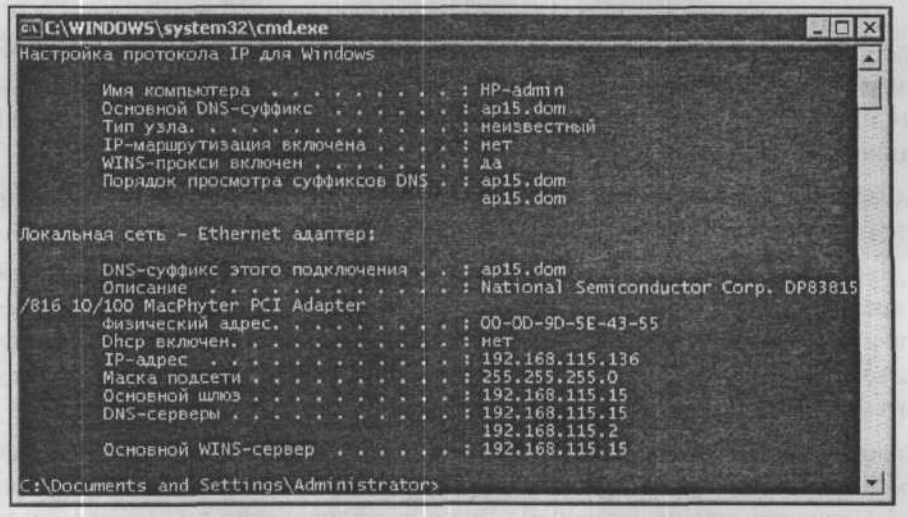

Рис. 1.13. Окно командной строки (результат выполнения команды `ipconfig /all`)

Для создания нового резервирования выберите в меню **Действие** окна **DHCP** пункт **Создать новое резервирование**. Перед этой процедурой посмотрите MAC-адрес той рабочей станции, для которой создается резервирование. MAC-адрес (MAC-addresses, Media Access Control layer addresses, адрес уровня доступа к среде передачи данных) — это 48-битный адрес, присвоенный изготовителем сетевой карте. DHCP может использовать этот адрес для идентификации машины, запрашивающей IP-адрес, при отсутствии других данных. Его потребуется указать без пробелов и дефисов при создании резервирования. MAC-адрес можно узнать, выполнив `cmd` и в окне командной строки набрав команду `ipconfig /all`. На экран будут выведены сведения о настройках IP-протокола (рис. 1.13), а в строке `Физический адрес` указан MAC-адрес компьютера.

Чтобы не было проблем

При самом удачном подборе программного и аппаратного обеспечения для вашей сети не представляется возможным эффективно их применять, если не обеспечены еще некоторые условия. Так, для обеспечения возможности удаленного управления вашей сетью необходимо, чтобы сеть имела выход в Интернет или была обеспечена возможность работы с помощью сервера удаленного доступа, установленного на одной из машин сети. Лучший вариант — это постоянное подключение к Интернету, именно такой вариант и будет далее рассматриваться. Конкретная реализация такого подключения зависит от ваших возможностей и набора услуг, предлагаемых поставщиками услуг Интернета в вашем регионе. В книге рассматривается в качестве основного варианта подключение через ADSL-модем, которое становится одним из самых распространенных способов подключения к глобальной сети даже в домашних условиях. Если у вас пока не организовано такое подключение, вы можете воспользоваться временно и обычным модемом. Но качество связи и скорость передачи данных в этом случае "оставляют желать лучшего", делая невозможным организовать полноценный доступ сколько-нибудь значительного числа пользователей сети к Интернету. Тем не менее модемное соединение может применяться для связи с вашей сетью извне.

Независимо от того, как организована политика распределения IP-адресов в вашей сети, компьютер администратора должен иметь постоянный IP-адрес. В случае с ADSL-подключением это позволит вам иметь полноценный доступ к сети Интернет, а также решить ряд других проблем.

Большинство пользователей вашей сети, включая в начале работы компьютер, проходят процедуру авторизации. При этом пользователь регистрируется в сети. Вам придется работать не только внутри вашей сети, но в автономном режиме. В этом случае вы не сможете зарегистрироваться в сети и получить

доступ к сеансу ее администратора. Чтобы не применять различные процедуры авторизации при включении компьютера в различных ситуациях вашей работы, следует всегда авторизоваться в качестве локального администратора компьютера. При этом операционная система Windows XP позволит вам запускать сетевые приложения и иметь доступ к сетевым ресурсам после авторизации в сети, если это необходимо. Соблюдение этого правила обеспечивает дополнительную защиту сети от несанкционированного доступа к критичным сетевым ресурсам с вашего компьютера, когда вы отошли от него, оставив включенным ваш сеанс. Только в отдельных случаях, например, при управлении компьютерами и сервером вашей сети средствами Windows, может потребоваться регистрация в качестве администратора домена.

Windows XP позволяет, выбрав **Запуск от имени...**, запустить (выполнить) любую программу от имени любого пользователя сети, если вам известен его пароль. Независимо от того, как вы зарегистрированы в данный момент в сеансе Windows, вы можете открыть окно файлового менеджера FAR от имени администратора сервера или домена и выполнить операции, доступные для этих пользователей.

Хотелось бы предостеречь от ошибки, которую нередко делают пользователи, неуверенно ориентирующиеся в каком-либо приложении. Вместо освоения этого приложения, они пытаются записать для себя точные пошаговые инструкции для выполнения той или иной задачи. В отдельных случаях это может быть оправдано. Но, если вы решили (решились) администрировать сеть, не надейтесь на пошаговые инструкции на все случаи жизни. Даже когда сеть будет настроена, вам неоднократно придется решать нестандартные задачи, для которых невозможно написать строгие инструкции. Что следует делать обязательно, так это протоколировать свои действия с обязательной отметкой о незавершенности или завершенности проводимых настроек. Говорят, что учеба на чужих ошибках малоэффективна, только свои синяки прибавляют разума. Но я попытаюсь все же рассказать об одной из моих ошибок, которая заставила поволноваться не только меня.

Ошибка

В 2002 году в нашей сети произошло знаменательное событие — сеть окончательно перешла на Windows 2000 Server. Если учесть, что до этого момента сервер работал не под Windows, к тому же был совсем не новым, возможности, появившиеся в сети с приобретением мощного современного сервера, казались безграничными. С огромным удовольствием я исследовал на практике возможности Windows 2000 Server. Организация учетных записей и политики доступа пользователей к серверу, возможность удаленного доступа через сервер терминалов, возможность организации общего доступа к Интернету, надежность и множество других особенностей и свойств новой системы делали работу увлекательной. Был один неприятный момент, который ограничивал возможности коллективного использования выхода в глобальную сеть — это доступ к Интер-

нету в режиме dial-up. Организация IP-адресов в сети не позволяла применить простые методы предоставления общего доступа к глобальной сети через новый сервер. Известный же своими возможностями и относительной сложностью настроек NAT (Network Address Translation, преобразование сетевых адресов) требовал выделения определенного пула адресов провайдером, что на тот момент было не реальным для нас. Тем не менее я прошел практически весь путь настройки общего доступа к Интернету через NAT и dial-up. Остановившись на отсутствии выделенных внешних адресов, я не стал возвращать настройки сервера в исходное состояние, поскольку они ничему не мешали, и сеть прекрасно работала.

Шло время, информационные технологии совершенствовались как в целом, так и в нашей отдельно взятой сети. Несмотря на отсутствие полноценного доступа в Интернет, потребовалось объединить сеть достаточно крупного удаленного офиса с нашей. Объединение проводили по выделенной модемной линии. С обеих сторон были поставлены маршрутизаторы с поддержкой необходимых протоколов, но... обнаружилось маленькое препятствие. При организации сетей об их объединении никто не задумывался, и в обеих сетях был применен стандартный для Windows адрес — 192.168.0.X с маской подсети 255.255.255.0. И наш сервер, и сервер удаленного офиса были контроллерами своих доменов. Они выдавали адреса своим клиентам и идентифицировали их при входе в сеть. Оба сервера совершенно обоснованно отказались видеть чужие компьютеры. Необходимо было кому-то решиться на смену IP-адресов в своей сети. Сама по себе процедура смены адресов не сложна, — если рабочие станции настроены на их автоматическое получение, достаточно изменить адрес сетевого адаптера на сервере. Вся работа должна занимать не более пяти минут.

В выходной день, когда в нашей сети работали лишь несколько человек, я решил выполнить эту несложную процедуру. Все рабочие станции предварительно были проверены на предмет автоматического получения адреса, и ничто не предвещало возникновения проблем. Но, не тут-то было.

Меняю адрес сетевого адаптера и проверяю работу сети, — ни одна рабочая станция не может войти в сеть. Вхожу в настройки сервера в раздел Active Directory. В нем должны находиться сведения обо всех пользователях, компьютерах и принтерах нашей сети. О, ужас! Active Directory в девственно чистом виде, — ни одной записи! Я начинаю в уме проигрывать сценарий восстановления записей. Около сорока пользователей, десяток компьютеров с новыми операционными системами, несколько принтеров, доступных для всей сети. Потребуется снова вводить данные о пользователях, назначать им пароли, регистрировать компьютеры.... Сколько придется потратить времени? Сколько придется выслушать "комплиментов" в свой адрес со стороны пользователей и руководства? Волосы на голове слегка шевелятся, на лбу выступает холодный пот.

Нет, надо взять себя в руки и внимательно проанализировать ситуацию. Возвращаю прежний адрес серверу, заглядываю в Active Directory — все пользователи на своих местах!

Повторяю замену адреса — Active Directory пуст. Возвращаю прежние настройки — все на своих местах. Куда пропадают записи, как их вернуть при новом адресе сервера? Перелистал все доступные материалы в бумажном и электронном виде, — ответов нет. Звоню знакомому специалисту по сетям. Через час он у меня в серверной. Сидим вместе около нового сервера, меняем и воз-

вращаем обратно старый адрес. Никаких идей. Вспоминаем про второй сетевой адаптер, имеющийся в этом сервере, присваиваем ему старый адрес, а рабочей сетевой плате даем новый. Заглядываем в Active Directory — все записи на своих местах! Казалось бы, можно оставить этот вариант и дать пользователям возможность работать. Но второй сетевой адаптер может потребоваться для решения каких-либо новых задач. Надо искать причину проблемы.

Прошло около четырех часов активного поиска причин неполадки. Просмотрены все лог-файлы системы и служб, проверены настройки всех применяемых в сети сервисов. Напрашивается вывод, что Windows подкинула нам очередной "глюк", для устранения последствий которого потребуется полная переустановка системы на сервере. Очень не хочется принимать такое решение. Тем более что система лицензионная, а большинство "глюков" проявляются во взломанных пиратских версиях. Сама операционная система никак не реагирует на неисправность, никаких сообщений о конфликтующих службах или программах нет. Принимается решение, — дополнительно привлечь интеллектуальные ресурсы. Организуем некое подобие телефонной конференции.

Проходит еще минут сорок, когда появляется предположение об установленной, но не применяемой службе, работа которой связана с доступом в Интернет...

Честно скажу, что мне стало бы стыдно, если бы я вспомнил о своих опытах с NAT. Но я о них забыл. Более того, в журнале обслуживания сервера записей не было, — я не записывал тогда изменения, которые не имели отношения к реальным проблемам и не были связаны с необходимыми изменениями настроек.

В конце концов была деинсталлирована служба маршрутизации и удаленного доступа со всеми ее настройками и ссылками на старые сетевые адреса. После этого можно было отключить и второй сетевой адаптер, сбросив его настройки. Сеть заработала в нормальном режиме, рабочие станции получили свои адреса и доступ к серверу, записи Active Directory вернулись на свои места.

"Любопытство — не порок...", но оплошность, допущенная мной во время экспериментов, привела к потере времени нескольких человек, потраченного на поиски моей ошибки.

Сети были объединены. Я стараюсь не вспоминать об этом случае, потому что мне стыдно. Пользователи не вспоминают, потому что ничего и не узнали о "боевом" выходном дне, а участники событий..., может быть, и вспоминают, но не напоминают об этом мне, — из вежливости.

Надеюсь, что приведенный пример поможет вам избежать подобных оплошностей, и вы не будете терять часы в поисках несуществующей проблемы в операционной системе.

Соблюдение лицензионной политики

К сожалению, до настоящего времени руководители многих предприятий (и не только руководители) не разделяют мнение разработчиков коммерческих программных продуктов, что за программы надо платить. Средства на приобретение вспомогательных программ часто получить сложнее, чем на

приобретение оборудования. В отдельных случаях ситуация упрощается ввиду наличия OEM[1]-версий программ, которые предустановлены на новых компьютерах (это относится и к операционной системе). В других случаях приходится искать выход, и как вариант, можно применять условно бесплатные или совсем бесплатные программы. Возможно, что они не обладают полнотой функциональности коммерческих разработок, бывает, что они несколько "сыроваты", но их применение позволяет добиться очень серьезных результатов, если перед "промышленным" применением вы внимательно протестируете их и определите тонкие места и подводные камни, которые следует обходить. В отдельных случаях приходится засучить рукава и самому администратору. Собственно, этим мы и будем заниматься при рассмотрении многих из приведенных в книге примеров.

Для большинства пользователей ПК в США (и многих других странах) вопроса: "Какой дистрибутив использовать, официально приобретенный или украденный?",— не существует. Закон этих стран охраняет права авторов и производителей программного обеспечения. По разным причинам в нашей стране нет строгого соблюдения авторских прав на программное обеспечение. Даже если сейчас вы — абсолютно легальный пользователь всех программных продуктов, включая и ОС, установленную на вашем компьютере, оглянитесь в свое прошлое: неужели вы ни разу не применяли программ, приобретенных на "пиратских" дисках, а может быть и "взломанных" самостоятельно? Не говоря о моральных и юридических аспектах нелегального использования программ, следует упомянуть о проблемах технических. Так, например, некоторые программы при запуске проверяют наличие работающих копий в сети. Если обнаружена копия с тем же регистрационным ключом, то программа сообщает об этом и не запускается. Кроме того, существуют сервисы, доступные легальным пользователям программ и ОС. Это и техническая поддержка, и бесплатное получение новых версий (не всегда), доступность некоторых услуг и даже бесплатных программ. На сайте Microsoft, например, можно найти программы, для бесплатного получения которых достаточно ввести регистрационный ключ вашей операционной системы. Например, по ссылке **http://www.microsoft.com/windowsxp/using/digitalphotography/photostory/default.mspx** можно загрузить полезную для создания фотопрезентаций программу. С ее помощью вы сможете подготовить обучающие материалы для пользователей и поместить их на внутреннем сайте своей сети.

Иногда возможно применение условно бесплатных версий программ, ограничение времени на бесплатное применение которых может составлять от 15 до 45 дней, чего обычно достаточно для выполнения весьма серьезной рабо-

---

[1] Original Equipment Manufacturer. — *Ред.*

ты, а также для оценки необходимости их приобретения. Некоторые программы бесплатны для отдельных категорий пользователей. Например, файловый менеджер FAR бесплатен для жителей бывшего СНГ.

Во всяком случае, применение лицензионных программных продуктов избавит вас от многих проблем, а иногда и поможет "подогнать" программу под свои требования. На собственном опыте я убедился, что многие производители программного обеспечения чрезвычайно внимательно относятся к своим легальным пользователям. Если программа или утилита предназначена для выполнения нужных, но немногочисленных задач, а вы, как легальный пользователь, вносите конструктивные предложения по улучшению функциональности программы, — разработчики обязательно примут ваши предложения. При этом вы будете одним из первых пользователей обновленной по вашему предложению и нужной вам программы.

Поэтому, приступая к использованию новой программы, внимательно ознакомьтесь с лицензионным соглашением.

Реальная сеть

Перед тем как приступить к рассмотрению примеров администрирования сети, давайте познакомимся с самой сетью, на основе которой собирались примеры.

В начале главы вы уже видели фотографии с фрагментами серверной комнаты. Думаю, что нет смысла показывать фотографии рабочих мест, поскольку компьютер — во всех случаях компьютер, какой бы модели он ни был, а на каком столе он стоит, мало кого интересует. Другое дело структура сети. Сеть создавалась не сразу, кое-что в ней сделано не совсем по правилам, что было вызвано обстоятельствами ее расширения. Вполне возможно, что и у вас могут сложиться ситуации, не позволяющие строго соблюсти все нормы при организации рабочих мест в сети. На примере этой сети вы сможете увидеть, какие решения возможны, а какие — нет.

Расположив рисунки фрагментов сети (см. рис. 1.14—1.16) в порядке возрастания нумерации, вы получите представление о структуре всей сети. С целью уменьшения размеров рисунков, на них изображены только основные компоненты сети. Некоторые подробности конструктивного исполнения, а также значительная часть рабочих станций не показаны. Тем не менее на рисунках достаточно информации для рассмотрения устройства конкретной работающей сети.

Следует обратить внимание на то, что все участки сети, требующие надежного функционирования независимо от колебаний напряжения в сети питания или кратковременных перерывов в электроснабжении, снабжены ИБП.

В серверной (рис. 1.14) к источнику бесперебойного питания подключены абсолютно все устройства. На других участках бесперебойным питанием обеспечены коммутаторы и рабочие станции, выполняющие наиболее важные функции. В идеальном варианте, конечно, следовало бы обеспечить бесперебойным питанием все устройства в сети, но приходится выбирать оптимальную пропорцию между затратами и потерями. Рассматривая необходимость установки ИБП, следует учитывать ущерб, который может нанести неожиданное выключение того или иного компьютера. Конкретное назначение рабочих станций на рисунках не указано, и вы сами сможете оценить необходимость наличия ИБП на участках своей сети.

Давайте проведем обзорную экскурсию по сети, показанной на рисунках.

В верхней части рис. 1.14 представлена серверная. На рисунке отсутствует рабочее место администратора, поскольку для его подключения нет каких-либо особых условий, особенно если это ноутбук. Но этот компьютер можно отнести к обычным рабочим станциям, имеющим выход в Интернет (думаю, вы не лишите себя такой привилегии). Главный сервер сети — это сервер под управлением Windows 2000 Server (на рис. 1.14 — **Сервер 2000**). К сети он подключен с помощью единственного сетевого адаптера. Второй сервер под управлением ОС Windows Server 2003 (**Сервер 2003**) имеет два сетевых адаптера, один из которых подключен к сети, а другой — к ADSL-модему (Asymmetric Digital Subscriber Line, асимметричная цифровая абонентская линия), дающему возможность пользователям сети подключаться к Интернету. IP-адреса серверов выбраны из S-диапазона (см. табл. 1.1). Оба сервера используют один монитор, одну клавиатуру и одну мышь, которые подключены к серверам через коммутатор. Это позволяет сэкономить не только на приобретении монитора, но и место в серверной. К серверной приходят две телефонных линии. Одна обычная, к которой подключен модем ADSL, а другая выделенная, — по ней осуществлена связь с другой локальной сетью. Эта связь обеспечивается обычным аналоговым модемом, который подключен к маршрутизатору, соединенному, в свою очередь, с сетью через коммутатор (**Коммутатор 1**). К тому же коммутатору подключены и серверы. Для увеличения числа точек подключения кабельных линий применен второй коммутатор. Необходимость его применения обусловлена только количеством выходящих из серверной кабелей. Возможно, что вам достаточно будет одного коммутатора, а в реальной сети, на основе которой делался этот рисунок, стоят три. От коммутаторов кабели расходятся по этажам здания, а также в другие строения, удаленные на значительное расстояние от серверной. На рис. 1.15 одна из линий подписана как **Длинная линия**. Это кабель, имеющий протяженность более 100 м. На рис. 1.16 можно увидеть, что он приходит к обычному хабу, который выполняет функцию усилителя, а далее кабель преодолевает еще сто метров, и снова установлен хаб, к которому подключены несколько компьютеров. Перед вторым хабом есть кабельная петля. Это

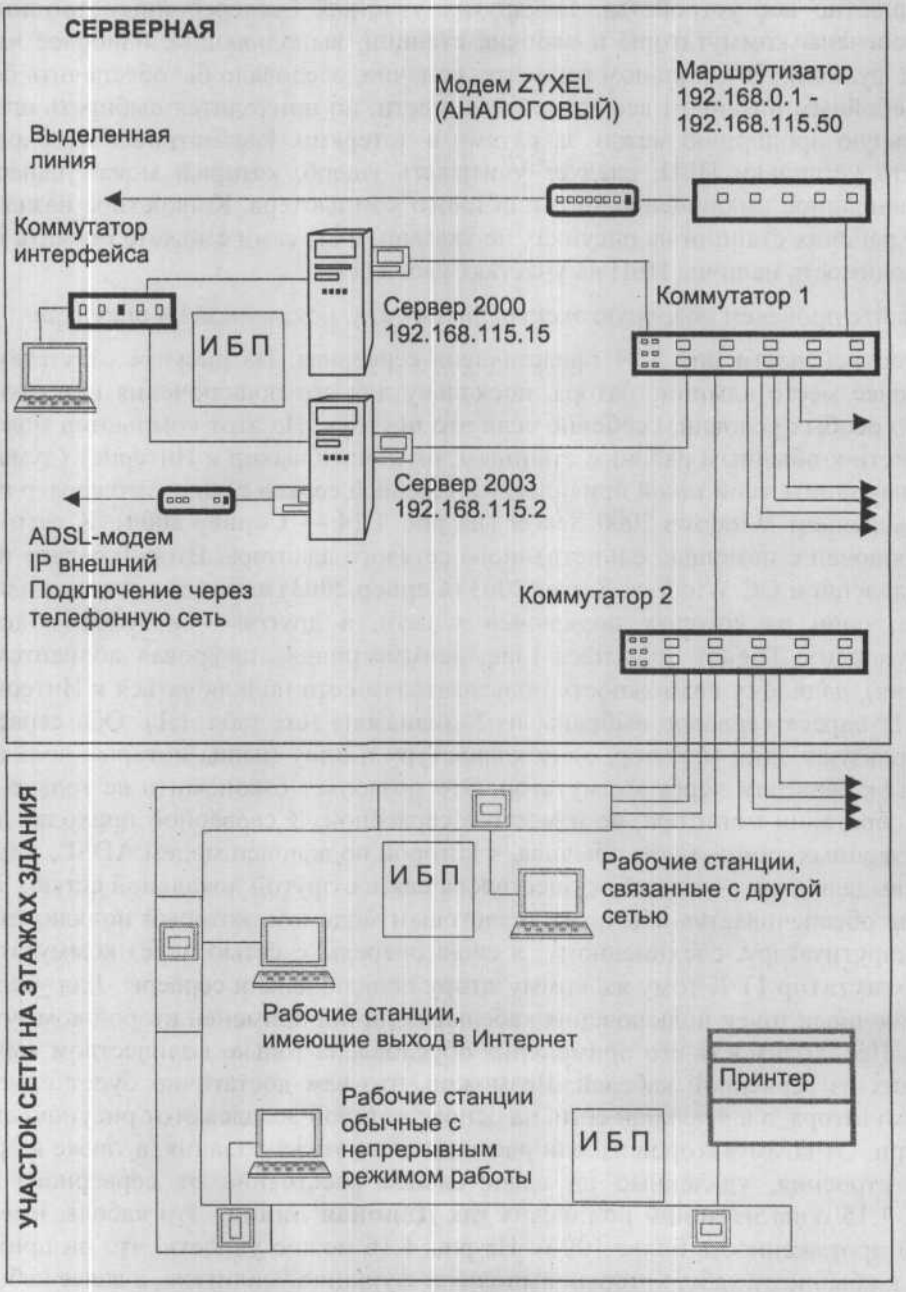

Рис. 1.14. Сеть (фрагмент 1)

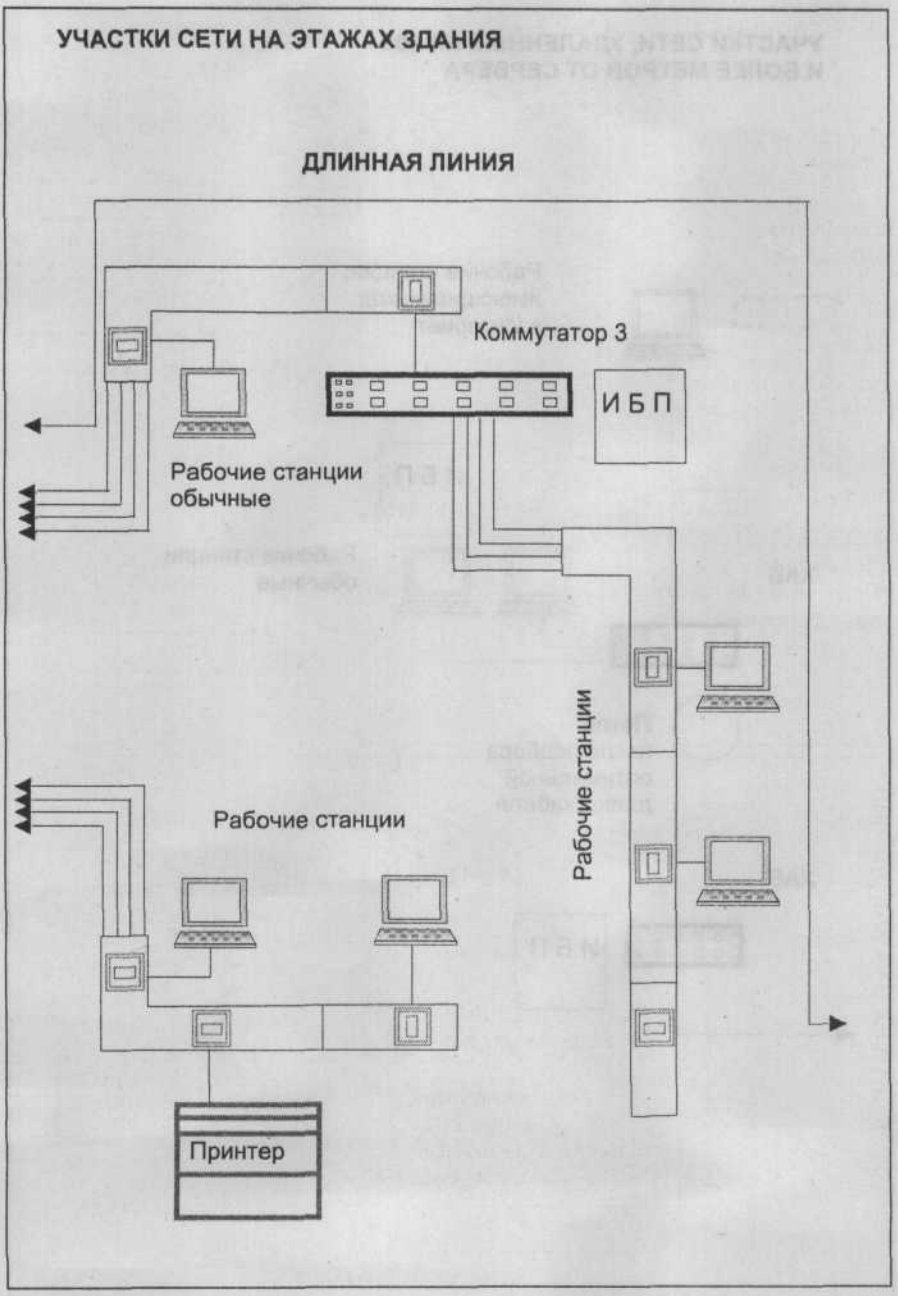

Рис. 1.15. Сеть (фрагмент 2)

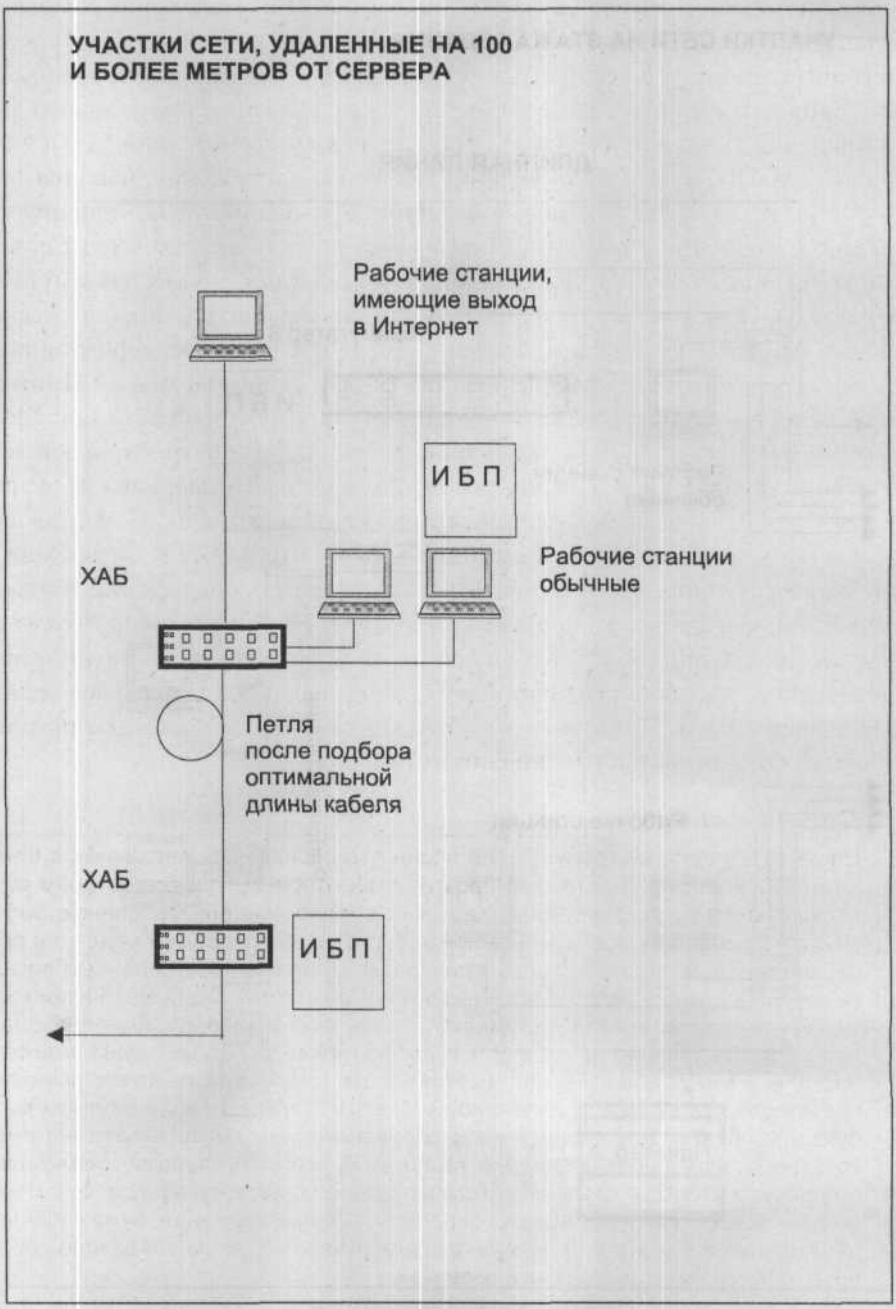

Рис. 1.16. Сеть (фрагмент 3)

некоторый запас кабеля, который позволяет подобрать его длину для достижения наилучшего качества связи. Если при первом включении компьютера наблюдаются проблемы со входом в сеть, кабель можно постепенно укорачивать (примерно по пятьдесят сантиметров за один раз), проверяя каждый раз связь. Скорее всего, отрезав не более 2,5 м, вы добьетесь нормального функционирования компьютера. Важно только, чтобы на пути прокладки такого длинного кабеля не встречались линии высокого напряжения, наводки от которых не позволят работать на такой линии. В большинстве помещений сетевой кабель уложен в короб с розетками. При недостатке точек подключения на других этажах могут устанавливаться дополнительные коммутаторы (**Коммутатор 3** на рис. 1.15), которые позволят включить в них еще несколько линий на этаже. Если применяются принтеры с принт-сервером, они подключаются как обычные компьютеры (на рисунках подписаны — **Принтер**). Других особенностей, кроме наличия длинной линии, у этой сети нет. Можно обратить внимание на то, что назначение рабочей станции никак не влияет на ее способ подключения к локальной сети. Поэтому, рассматривая далее работу в сети, мы не будем возвращаться к ее устройству, способам прокладки кабеля и подключения рабочих станций. Важно, чтобы все работы были выполнены качественно, что обеспечит надежность всех соединений и отсутствие проблем, связанных с плохими контактами. Не менее важно, чтобы правильно были выбраны места прокладки кабеля. Не вдаваясь в технические и теоретические подробности, расскажу о том, как прокладывалась длинная линия в нашей сети. Возможно, что этот рассказ будет полезным примером для оценки возможностей расширения сети.

Длинная линия

Наша сеть росла не сразу. После первых модернизаций, связанных с появлением ОС Windows 95, это был просто компьютерный класс, в котором стояли несколько компьютеров Vectra. Каждый день компьютеризированные рабочие места встречали и провожали своих операторов, которые имели где-то в других кабинетах свои рабочие столы, заваленные бумагами, заставленные письменными приборами, а около столов — корзины для бумаг. Сюда же они приходили вкусить несколько минут "безбумажной" технологии, которая позволяла, заполнив несколько электронных форм и выбрав свой "заветный" пункт меню, еще несколько минут завороженно смотреть, как матричный принтер, повизгивая, покрякивая и постукивая, аккуратно складывает гармошку из нескольких метров бумажной ленты, заполненной цифрами, фамилиями и отдельными знаками, из которых складывались огромные таблицы. С этими таблицами, фамилиями и цифрами операторы уходили из компьютерного класса, превращаясь в обыкновенных конторских работников, переписывавших с длинной бумажной ленты фамилии и цифры в толстые журналы или отчеты, которые следовало представить к определенному сроку руководству.

Но так продолжалось недолго. Пришло время, когда конторские работники потребовали установить компьютеры Vectra на их письменные столы. Для этого

потребовалось тянуть через коридоры и этажи к их кабинетам кабели. Через несколько недель в классе осталось три компьютера, которые не сложно было бы переместить в кабинеты конторских работников, но этих работников было более десятка, и решить, кому же из них больше нужен компьютер Vectra на рабочем столе, не представлялось возможным. Пришлось приобретать новые компьютеры. С этого момента сеть начала разрастаться со скоростью выделения финансовых средств на развитие информационных технологий. Появились заявки от конторских работников, постоянное место работы которых находилось в соседнем здании. Пройдя размеренным шагом от сервера до одного из таких рабочих мест, мы обнаружили, что размеренных шагов получилось около двухсот.

Применяя навыки, полученные, вероятно, на сборах скалолазов, наши электрики довольно быстро дотянули кабель до соседнего здания. Прикрепленная к проволоке, натянутой между зданиями, и помещенная в гофрированный рукав, воздушная часть линии выглядела прекрасно и не вызывала сомнений в своей работоспособности. Но было пройдено лишь пятнадцать-двадцать метров....

Оставалось пройти еще более ста пятидесяти метров. Понятно было, что кабель такой длины не сможет обеспечить нормальную связь рабочих станций с сервером. Пройдя по предполагаемой трассе кабеля, мы выбрали места для установки двух хабов. Здание, под потолком которого намечено было проложить кабель, было опутано множеством проводов разнообразного назначения. Несмотря на то, что электрики старательно пытались обойти все участки, на которых сетевой кабель мог бы пройти рядом с силовой проводкой, оказался всего один такой короткий отрезок трассы, где расположить кабели на достаточном расстоянии друг от друга не удалось. Подключив хабы и рабочую станцию, мы попытались зарегистрироваться в сети. Было сделано несколько попыток, несколько раз перепроверены настройки компьютера, но вход в сеть не удался. Пытаясь понять причины неудачи, мы решили провести инструментальный контроль качества сигнала. Настоящих тестеров для контроля качества сетевой связи у нас не было. Единственное, что было в нашем распоряжении, — это команда ping, индикаторы на хабах и осциллограф, оставшийся с тех пор, когда компьютеры еще можно было ремонтировать своими силами. Команда ping давала весьма нестабильный результат, индикатор коллизий на промежуточном хабе горел почти постоянно, а после подключения осциллографа к выходу хаба на экране были сплошные наводки от питающей сети, украшенные помехами от ламп дневного света и прочего оборудования, работающего в здании. Приговор проложенной линии был вынесен. Кабель был снят и переложен по наружной стене здания. На это потребовалось еще два дня.

После окончания работ по прокладке кабеля мы продолжили тестирование. Проверка связи на промежуточном хабе дала прекрасный результат. От сервера до этого хаба было около ста десяти метров. Второй участок был не намного короче. Первая попытка входа в сеть оказалась неудачной. Я не помню, откуда я взял тогда эту информацию, но уже и по опыту знал, что в длинном кабеле есть резонансные явления, и качество связи может зависеть от кратности длины кабеля некоторой величине. Кабель еще не был окончательно закреплен около второго хаба, и его конец имел несколько большую, чем необходимо, длину. Укорачивая кабель по пятьдесят сантиметров за один раз и проверяя результат, на третий раз мы добились явного улучшения связи.

Дополнительно переключив порт коммутатора в серверной на скорость 10 Мбит/с, мы получили абсолютно стабильную связь. Более того, от второго хаба позднее был проложен еще один кабель длиной около шестидесяти метров. Компьютер, подключенный к самому удаленному участку сети, сразу зарегистрировался в сети.

Теперь наша сеть разрослась. Организованы линии связи, работающие на основе самых современных технологий, включая оптоволоконную. Но эта длинная линия общей протяженностью более двухсот метров работает до сих пор. Конечно, если следовать веяниям времени, ее следовало бы заменить на более современное оптоволокно. Но попробуйте сравнить цену двухсот метров витой пары и двух хабов с ценой оптического кабеля, двух оптических трансиверов, и цену работы по монтажу оборудования. Да и устраивает пока всех эта длинная линия.

А конторские работники теперь стали настоящими пользователями ПК, технология их работы приближается к действительно безбумажной. Они мастерски оперируют с сетевыми ресурсами и не имеют никакого представления о том, по каким путям их компьютеры добираются до этих ресурсов. Но им это и не интересно...

Начиная работу по подготовке средств администрирования локальной сети, следует отметить для себя особенности, которыми можно охарактеризовать сервер сети, и отличия сервера от рабочей станции, которые накладывают некоторые ограничения на свободу наших действий при работе с этими компьютерами. Специфические задачи сервера требуют от него практически непрерывной работы. Это значит, что перезагрузки и выключения сервера чаще всего недопустимы. Тем не менее изредка такие процедуры требуются в процессе работы администратора сети. Следует определить некоторые небольшие интервалы времени, в течение которых перерывы в работе сети нанесут наименьший ущерб работе пользователей, и приурочивать к ним перезагрузку или выключение сервера. Если пользователи сети в это время могут работать в сети, то они должны знать, что это период риска потерять не сохраненные данные или невозможности использовать некоторые сетевые сервисы. Но периоды эти должны быть максимально сокращены. Если ваша сеть работает в организации, то лучше всего такие "непопулярные меры" предпринимать в выходные дни. Тем не менее, даже в отведенное для этих процедур время, необходимо проверить наличие в сети пользователей и оповестить их о предполагаемом перерыве в работе сервера. Если в вашем распоряжении не один сервер, то можно повысить безотказность сети, настроив дублирование некоторых функций основного сервера. Например, совсем не сложно на втором сервере установить службу DNS, скопировав зоны просмотра с основного сервера и настроив синхронизацию с ним. При этом рабочие станции пользователей должны иметь возможность обратиться к этому серверу при необходимости, т. е. он должен быть указан в них как альтернативный.

Сколько-нибудь значительный опыт работы с любым компьютером обычно приводит к убеждению, что следует более или менее регулярно сохранять резервные копии данных. Для рабочей станции это чаще всего выполняется правильно, — данные архивируются на внешний носитель (дискета или диск CDRW). Когда дело доходит до работы с сервером, то нередко его надежность "гипнотизирует" администратора. Архив данных создается на самом сервере, да еще на системном диске. Несмотря на очень высокую надежность сервера, вероятность отказа всегда существует, даже если реально в вашей практике отказа с потерей данных не происходило. Быть готовым к такой ситуации следует постоянно.

Авария

Был уже поздний вечер, когда мне позвонил администратор одной из сетей, с работой которой я был хорошо знаком. Оказалось, что уже с середины дня пользователи его сети не могли в ней зарегистрироваться, сервер отказался работать. Мы перезванивались на протяжении нескольких часов, до тех пор, пока работа сети не восстановилась. Компьютер, исполняющий роль сервера, работал нормально, но система Windows 2000 Server без видимых на тот момент причин перестала загружаться. Администратор терялся в догадках. По его словам, в процессе загрузки система сообщала о разрушении каталога Active Directory. Попытка восстановить каталог, предложенная самой системой, к успеху не привела. Архива системы или архивного образа диска не создавали...

Диск этого сервера был разбит на три раздела, на одном из которых была установлена система. За полдня борьбы с проблемой не удалось найти ее решения. Все шло к тому, чтобы установить систему заново. Уже поздно вечером была сделана попытка установить вторую систему на свободный раздел, чтобы попытаться увидеть проблему в системе сервера...

Первое, что было обнаружено при осмотре из второй системы, — на диске полностью отсутствовало свободное место!

Архивы данных, как выяснилось, создавались на системном разделе, и они "съели" все свободное место. При этом восстановление системных баз данных, таких как каталог Active Directory, оказалось невозможным, несмотря на попытки системы выполнить эту процедуру.

Пришлось заново вносить учетные записи пользователей и определять их права. Но утром выяснилось, что не работают DNS-сервер и DHCP-сервер! Точнее, они работают неправильно, а пользователям сети, тем временем, требовалось срочно закончить начатую работу.

В конце концов, к обеду следующего дня удалось заставить рабочие станции подключиться к серверу. Подробности всех проведенных манипуляций описывать не буду, поскольку все они позволили лишь на некоторое время решить проблему для завершения работы пользователей.

Впереди, все же, была полная переустановка сервера...

Вот так отразилось на состоянии сети создание архивов данных на системном диске при отсутствии контроля над их размером.

Единовластие

"У семи нянек дитя без глазу". Эта старинная поговорка определяет и основное правило администрирования компьютерной сети. Управлять сетью должен один администратор. Конечно, могут быть помощники, которым даны права на управление отдельными задачами по администрированию сети, но за все несет ответственность Администратор. В состав пользователей Windows 2000 Server, например, заранее включены несколько групп пользователей, наделенных определенными правами, и только один Администратор имеет неограниченные права для управления сервером и сетью. Администратор вправе добавить любое число пользователей с правами администратора, но обычно этого делать не следует. Последствия коллективного администрирования могут быть весьма плачевными, поскольку даже при высокой квалификации многочисленных администраторов их действия могут быть не согласованными и противоречащими одно другому. А ошибки, от которых никто не застрахован, могут привести к непоправимым ситуациям. Если сеть растет, и в домене появляются несколько подсетей, то у каждой подсети должен появиться свой администратор. Администратор домена согласовывает свои действия с администраторами отдельных служб и систем. До тех пор, пока у вас один домен и одна небольшая сеть, вы должны быть единственным администратором вашей сети. Работы по обслуживанию сети и компьютеров обычно носят более или менее периодический характер. Техническое обслуживание сервера и компьютеров сети, архивирование важных данных, требующих хранения, обслуживание базы данных (если применяется), удаление и добавление учетных записей пользователей и компьютеров сети и другие работы по обслуживанию сети желательно протоколировать. Проблемы, неожиданно возникшие в какой-то момент в сети, можно решить оперативно, если быстро найден источник проблемы, а в этом могут помочь записи обо всех изменениях, проводимых в сети. Например, замена сетевой карты на клиентском компьютере иногда приводит к нарушению работы базы данных MS Access. Если у вас в хронологическом порядке регистрируются изменения, произошедшие в сети, то причина проблемы может быть выявлена при анализе этих записей. Все изменения, которые вносят пользователи на своих компьютерах (если им это разрешено), должны быть согласованы с администратором.

Удобнее всего вести записи в специально отведенном журнале. Если есть абсолютная уверенность, что всегда будет доступен какой-либо компьютер для чтения электронного дневника, то бумажный журнал можно и не делать. Но каждый раз после внесения записей следует сохранять не менее двух копий дневника на съемных носителях. Форма дневника при этом должна быть такой, чтобы при необходимости можно было распечатать его часть или весь дневник.

Дневник администратора

Форма дневника может быть произвольной. Но должны быть предусмотрены разделы по видам работ, а также справочный раздел с описанием клиентских рабочих станций, аппаратного и программного обеспечения сети, схемой сети с указанием особенностей кабельной системы на различных участках. Затраты времени на ведение такого дневника оправдают себя при устранении сетевых неполадок, особенно в случаях, когда заниматься этим придется новому администратору. А смена руководства сети, как и смена любого другого руководства, вполне возможна.

Дневник может содержать следующие разделы.

1. Работы по обслуживанию сервера (программное обеспечение и аппаратная модификация, изменения разрешений) (табл. 1.2).

   Содержит записи обо всех изменениях, производимых на сервере. В хронологическом порядке помещены сведения обо всем, что вами или с вашего ведома делалось на сервере.

2. Работы по обслуживанию применяемого программного комплекса (табл. 1.3).

   Содержит записи об установке и модификации прикладного программного обеспечения.

3. Работы по обслуживанию сети (кабельная система и оборудование) (табл. 1.4).
4. Пользователи (закрепление пользователей за компьютерами) (табл. 1.5).
5. Компьютеры сети (краткая характеристика и сведения о модификации) (табл. 1.6).

   Позднее мы рассмотрим вариант ведения этого раздела, который не доставит много хлопот.

6. Схема сети (рис. 1.14—1.16).

   Рисунок, приведенный при описании примерной сети, может быть основой для составления схемы вашей сети.

Таблица 1.2. *Работы по обслуживанию сервера*

Дата	Время	Проблемы	Сделано	Результат
19.06.2003	12:53	Не используемые учетные записи	Удалены пользователи User1, User2 User3	+
19.06.2003	16:00—16:30	Сбой при настройке нового программного обеспечения	Перезагрузка	+

Таблица 1.2 (окончание)

Дата	Время	Проблемы	Сделано	Результат
20.06.2003	21:00	Права пользователей	Установлены права на DIR DOC для пользователей User25 и User15	+
21.06.2003	22:15—23:50	Внеплановое отключение в связи с перебоями электроснабжения	Сервер запущен	+
21.06.2003	23:00	Модификация	Замена CDROM (установлен CDRW)	+

Таблица 1.3. Работы по обслуживанию программного комплекса

Дата	Время	Проблемы	Сделано	Результат
15.06.2003	09:15	Замена программных модулей	Заменены abc.exe на версию от 10.06.2003	+
19.06.2003	15:00	Не работает abc.exe в режиме A	Настройка параметров запуска	– (сбой def.exe в режиме B)
19.06.2003	16:35	Не работает def.exe в режиме B	Настройка параметров доступа	+

Таблица 1.4. Работы по обслуживанию сети

Дата	Время	Проблемы	Сделано	Результат
12.06.2003	10:15	Не обеспечивается 100 Мбит для Comp DEN	Замена устаревшего (к3) кабеля на (к5) 25 м	+
19.06.2003	15:00	Добавление рабочей станции Comp18	Подключение	+

Таблица 1.5. Пользователи и компьютеры

Дата	Компьютер	Пользователь	Должность	Имя для входа
01.03.2003	DEN (в отделе N)	Иванов Иван Иванович (User17)	Программист	Prog

Таблица 1.5 (окончание)

Дата	Компьютер	Пользователь	Должность	Имя для входа
01.03.2003	GSM (в отделе L)	Петров Петр Петрович (User14)	Начальник отдела	PPP

Таблица 1.6. Компьютеры сети

Дата	Компьютер	Система
Подключен 01.03.2003	Computer System	Win98SE
Сведения: Идентификация Comp1, Сетевая карта — (тип 1), Office 2000, IE6 IP статический 192.168.0.109		
Модификации		
15.05.2003	Обновление Office 2000	
20.06.2003	Замена сетевой карты (тип 1 на тип 2)	

В любой момент времени, имея такой дневник, вы сможете оценить ситуацию и оперативно разобраться в причинах неполадок, если они вызваны вашими действиями или согласованными с вами действиями пользователей. Форма дневника может отличаться от рассмотренной, возможно добавление каких-либо разделов, если это необходимо.

Последняя рекомендация

Каждый компьютер вашей сети в своих учетных записях имеет пользователя с правами администратора. Необходимо, чтобы вы, как администратор сети, также были администратором каждой рабочей станции. Для этого следует произвести несложную процедуру добавления пользователя.

1. Войдите в систему рабочей станции ее администратором.
2. Откройте **Учетные записи пользователей** (рис. 1.17).
3. Нажмите кнопку **Добавить**.
4. В появившемся окне (рис. 1.18) введите имя учетной записи администратора домена и имя домена.
5. Если вы не помните этого имени (или требуется разрешить доступ к компьютеру для другой учетной записи), нажмите кнопку **Обзор**.

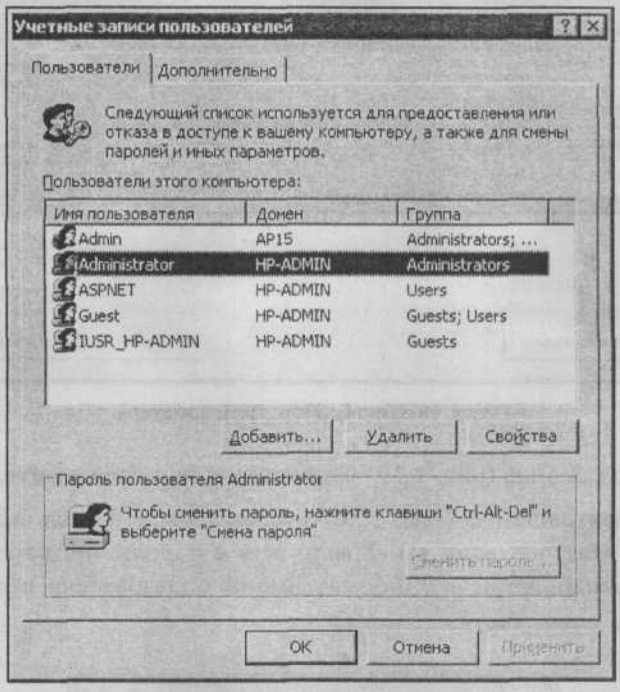

Рис. 1.17. Учетные записи пользователей

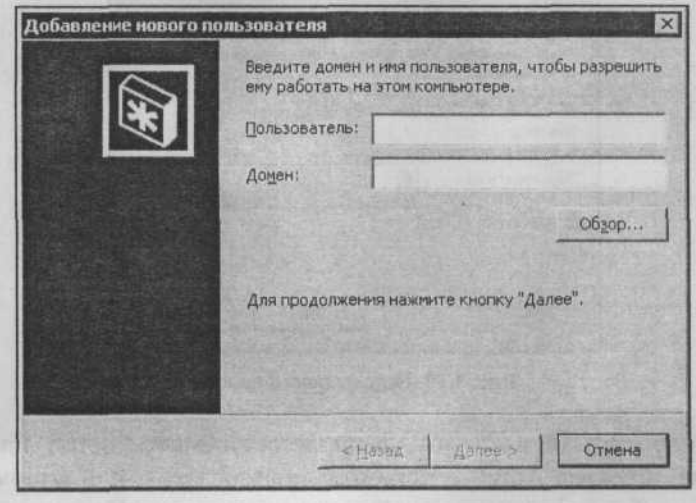

Рис. 1.18. Добавление нового пользователя

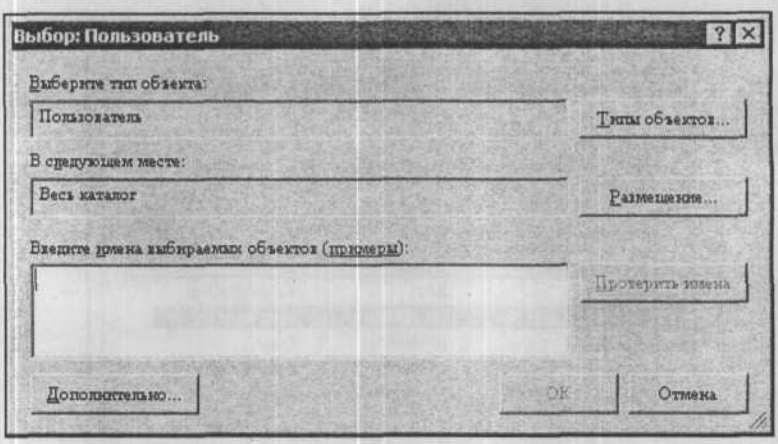

Рис. 1.19. Окно **Выбор: Пользователь**

6. В открывшемся окне (рис. 1.19) нажмите кнопку **Дополнительно**.
7. Появится приглашение (рис. 1.20) ввести имя и пароль администратора домена (на этот раз, если вы забыли имя и пароль, придется его искать в своих секретных записях). Формат имени пользователя в данном случае `<имя_домена>\<имя_учетной записи>`.

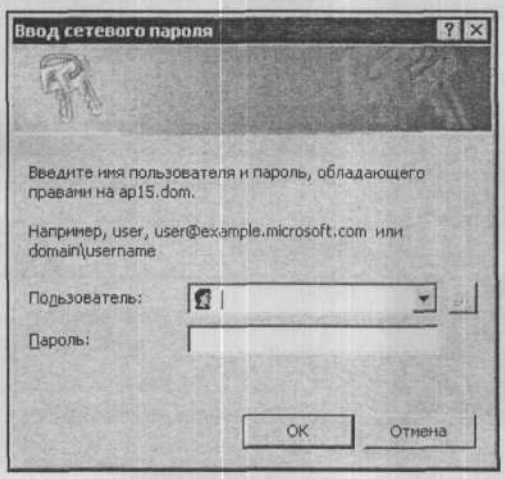

Рис. 1.20. Ввод сетевого пароля

8. В открывшемся окне выбора пользователя нажмите кнопку **Размещение**, и в дереве объектов найдите искомого пользователя, или в поле **Имя** введите первые буквы имени учетной записи, и нажмите **Поиск**.
9. В списке учетных записей выберите необходимую вам.

10. Нажмите два раза **OK**, затем — кнопку **Далее**.
11. В окне **Добавление нового пользователя** выберите его права для данного компьютера.
12. Нажмите кнопку **Готово** и закройте все окна.

Все, администратор домена добавлен в число администраторов компьютера.

После добавления администратора домена в число администраторов каждой рабочей станции, во многих случаях не потребуется подходить к ним для решения текущих проблем.

"Секретные" адреса

Однажды, когда я показал одну из своих статей очень серьезному специалисту по сетевым технологиям, мне было высказано замечание, касающееся публикации реальных IP-адресов сервера и рабочих станций. Когда я спросил его, чем же это грозит этой сети, — специалист ненадолго задумался и, немного удивившись своим мыслям, произнес: ничем. На самом деле, и в форумах в Интернете, и в публикациях можно найти массу примеров, когда реальный IP-адрес компьютера, находящегося в локальной сети, скрывают (замазывают, искажают, просто не показывают). Не знаю, чем это можно объяснить, но то, что это никак не прибавляет защищенности сетям, абсолютно точно. Пожалуй, номер квартиры, в которой я живу, названный где-нибудь в Лондоне, откроет обо мне больше информации, чем IP-адрес моего компьютера в локальной сети, опубликованный во всех газетах города. Посмотрите на IP-адрес вашего компьютера, если он находится в локальной сети предприятия. Скорее всего, он начинается выражением 192.168. С несколько меньшей вероятностью можно утверждать, что следующая цифра в этом адресе — 0. Остается определить последнее число, вариантов которого двести пятьдесят четыре. Сколько таких сетей в вашем городе? Но дело не только в том, что значительная часть сетей имеет одинаковые IP-адреса. Пусть даже ваш сервер имеет IP-адрес, смотрящий в вашу сеть, совершенно нестандартного вида. Если этот адрес не виден из Интернета, вы можете сообщить его кому угодно, причем совершенно безопасно для вашей сети. В то же время, если вы тщательно скрываете свои внутренние адреса, но посылаете электронные письма, то уже есть возможность определить ваш внешний адрес, а в документах MS Word можно увидеть пользователя, создавшего их, имя вашего домена. Но до сих пор эта информация не помогала проникнуть в нормально защищенную сеть. А если вы не позаботились о защите своей сети, то, получив ваше письмо, какой-нибудь хакер, и не только хакер, а школьник, увлекшийся информатикой, не только узнает ваши внутренние адреса, но и проникнет к вам в сеть (хорошо, если только из любопытства).

Но при правильно организованной сети даже передача вашего внешнего адреса вместе с внутренними IP-адресами не повлечет негативных последствий. Для большинства локальных сетей сокрытие от окружающих своих IP-адресов бессмысленно. Лучше позаботиться о нормальной защите сети от несанкционированного доступа как изнутри, так и снаружи. Другое дело, если вся ваша сеть имеет зарегистрированные в Интернете адреса, и каждая рабочая станция видна из любой точки мира... но, такой вариант построения сети не только маловероятен, но дорог и не рационален.

На этом завершим наши предварительные замечания и рекомендации. Мы познакомились в общих чертах с сетью, которая, вполне вероятно, во многом похожа на вашу. Возможно, наоборот, — ваша сеть в скором времени станет похожей на эту. В следующих главах мы рассмотрим работу администратора сети, связанную с поддержанием ее нормальной работы, а также способами рациональной организации этой работы.

ГЛАВА 2

Управление сервером и организация сервисов

Вооружившись основными представлениями о работе администратора сети, мы можем приступить к рассмотрению собственно приемов и методов администрирования. В конце первой главы было рекомендовано вести дневник администратора. В этом дневнике будут собираться сведения о событиях, которые происходят по вашей инициативе. Но в вашей практике обязательно встретятся случаи, когда этих сведений будет недостаточно для принятия решения о дальнейших действиях при возникновении той или иной проблемы. К счастью, сама операционная система сервера располагает средствами протоколирования практически всех происходящих в ней событий, которые могут иметь отношение к нарушению работоспособности сервера или отдельных приложений. Для этих целей предназначены системные журналы. Эти журналы могут быть очень полезным дополнением к вашему дневнику, когда потребуется докопаться до сути возникшей проблемы.

Системные журналы — информация для администратора

Каждый системный журнал несет в себе информацию о том виде событий, для которых он предназначен. Не всегда записи этих журналов можно понять с первого раза. Если событие содержит информацию об ошибке, то для известных ошибок приводится краткое описание и идентификатор. По идентификатору можно найти более подробное описание в базе знаний Microsoft, хотя найти такое описание удается не всегда. Несмотря на то, что Microsoft активно собирает сведения об ошибках ОС и программ, причины части из них остаются неопределенными. Это и понятно. Есть ошибки, вызываемые действиями администратора, которые не предусматривались разработчиками системы. Но даже в этом случае, сопоставив записи в дневнике с записями в

системных журналах, легче сориентироваться в ситуации и локализовать проблему.

Системные журналы существуют не только в серверной операционной системе, но и во всех современных локальных ОС. Поскольку проблемы в сети могут быть вызваны проблемами на рабочей станции, имеет смысл заглядывать и системные журналы компьютеров пользователей сети. Во всех операционных системах Windows, начиная с версии 2000, системные журналы можно просмотреть, открыв закладку **Event Viewer** (Просмотр событий).

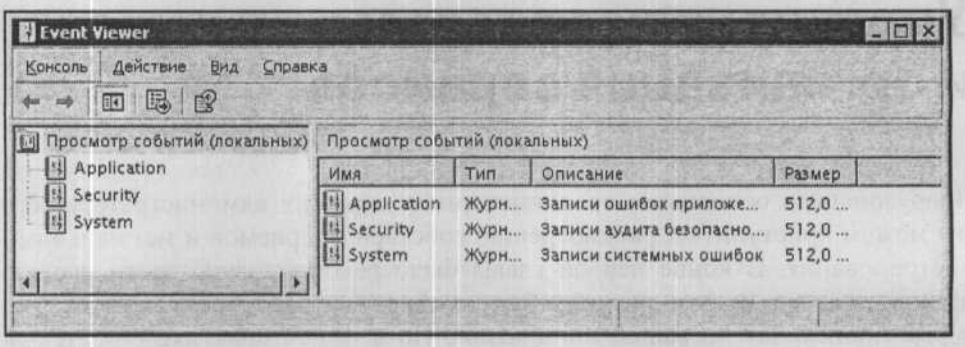

Рис. 2.1. Просмотр событий в окне **Event Viewer**

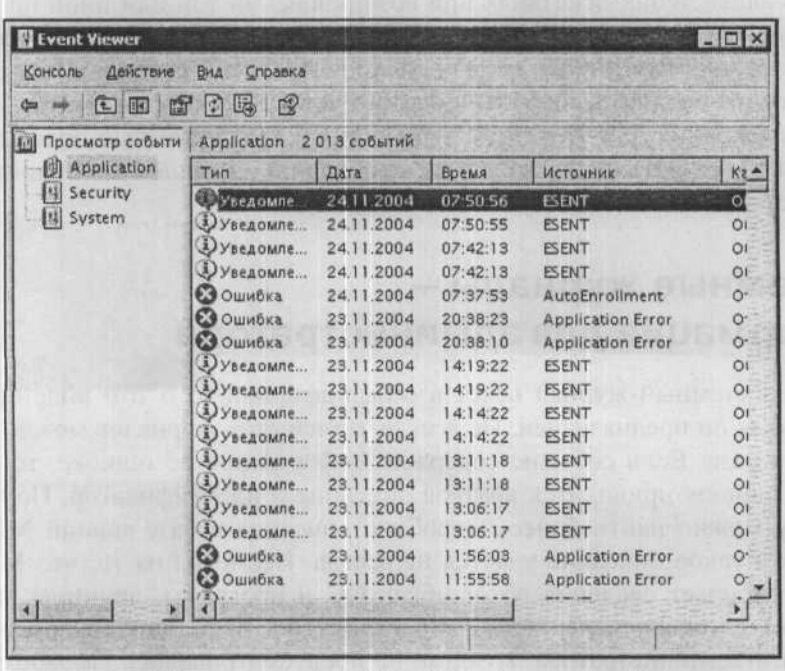

Рис. 2.2. Журнал приложений (**Application**) в окне **Event Viewer**

В ОС, предназначенных для рабочих станций, в автоматическом режиме ведутся три журнала (рис. 2.1). Это журнал системы (System), журнал приложений (Application) и журнал доступа (Security).

Любой журнал можно просмотреть, выделив его. При этом в правой части окна появится список сообщений из этого журнала (рис. 2.2).

Сообщения имеют три типа: уведомления, предупреждения и ошибки. Для просмотра любого сообщения следует посмотреть его свойства (рис. 2.3).

В окне свойств события можно прочитать имеющуюся о нем информацию и, при необходимости, по имеющейся в окне ссылке подключиться к базе знаний Microsoft для получения более подробных сведений. С помощью кнопок со стрелками можно переходить от одного сообщения к другому в пределах журнала.

На сервере журналов больше. Важнейшие для обеспечения работы сети службы имеют свои журналы.

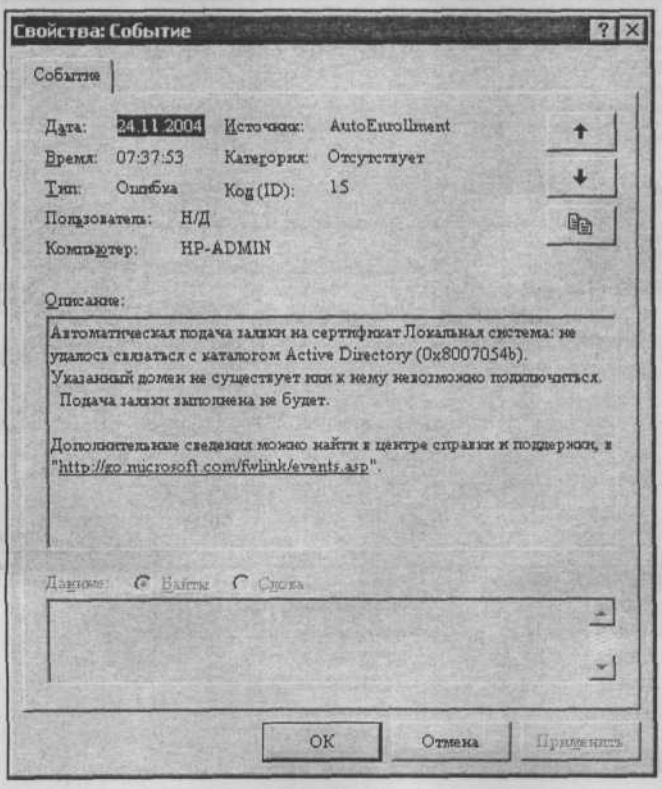

Рис. 2.3. Свойства события

Не стоит подходить к серверу

Для того чтобы просмотреть журналы событий на сервере, можно подойти к нему и аналогично уже рассмотренному способу открыть нужный журнал. Но наша задача — упростить работу администратора. Удобнее просматривать информацию в нескольких окнах на одном компьютере, чем ходить от машины к машине, запоминая, то, что вы увидели. Ваш компьютер (если на нем установлена ОС Windows XP) позволяет просмотреть журналы событий *на любом компьютере сети!* Для этого нужно совсем немного. Настраивая для работы в сети компьютер, необходимо в число его локальных администраторов включить администратора домена. Как это сделать, мы уже рассмотрели в первой главе.

Откройте **Event Viewer** (Просмотр событий) от имени администратора домена. Для этого в контекстном меню большинства ярлыков в Windows XP есть

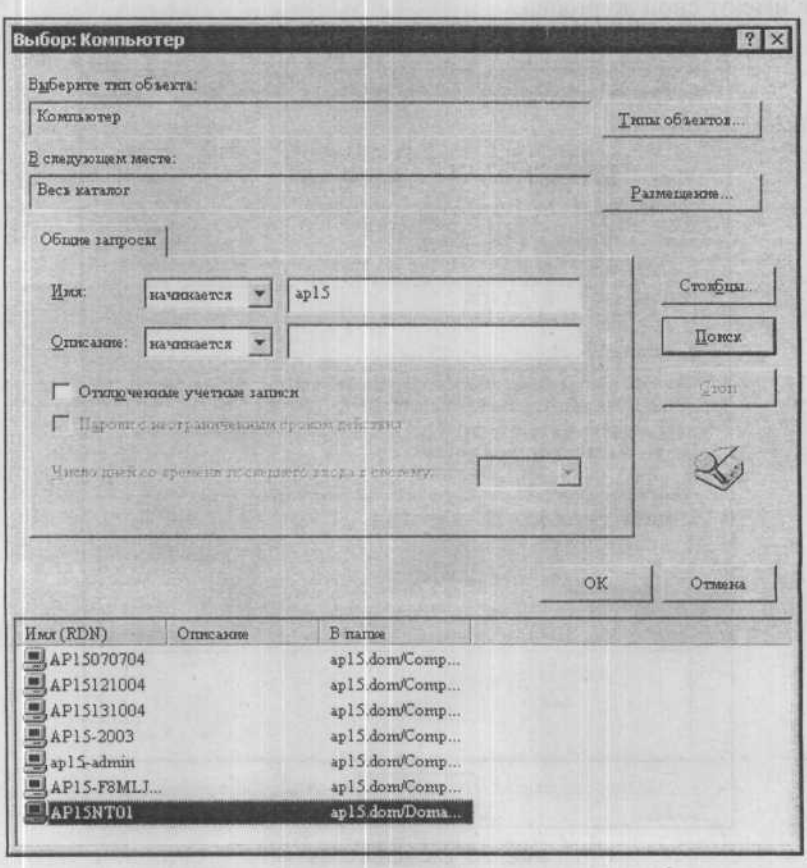

Рис. 2.4. Окно **Выбор: Компьютер**

соответствующий пункт. В окне просмотра событий (см. рис. 2.1) нажмите кнопку **Действие** и выберите опцию **Подключиться к другому компьютеру**. Откроется окно выбора компьютера (рис. 2.4).

Введя первые буквы имени компьютера, вы получите список компьютеров, в котором необходимо выбрать искомый сервер (но можно и другой компьютер, если необходимо).

Теперь в текущем окне, где появилось имя выбранного компьютера (рис. 2.5), нажмите **OK**. В следующем окне (рис. 2.6) снова нажмите **OK**.

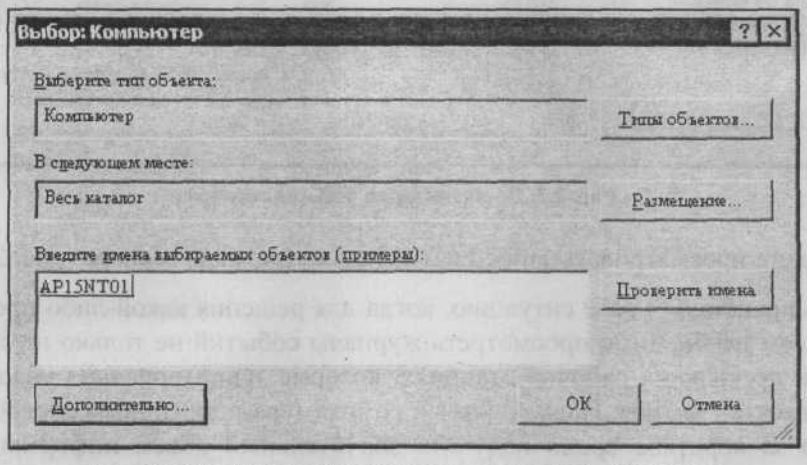

Рис. 2.5. Окно **Выбор: Компьютер** после завершения выбора

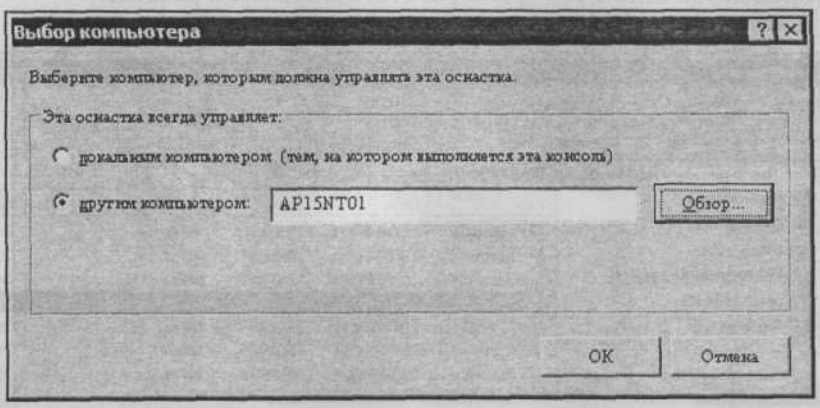

Рис. 2.6. Окно **Выбор компьютера** (после завершения выбора)

Если имя компьютера известно и нет сомнений в его правильности, то можно сразу ввести его в соответствующее поле окна **Выбор компьютера**.

Теперь откроется знакомое окно просмотра событий, но подключено оно будет к серверу (рис. 2.7).

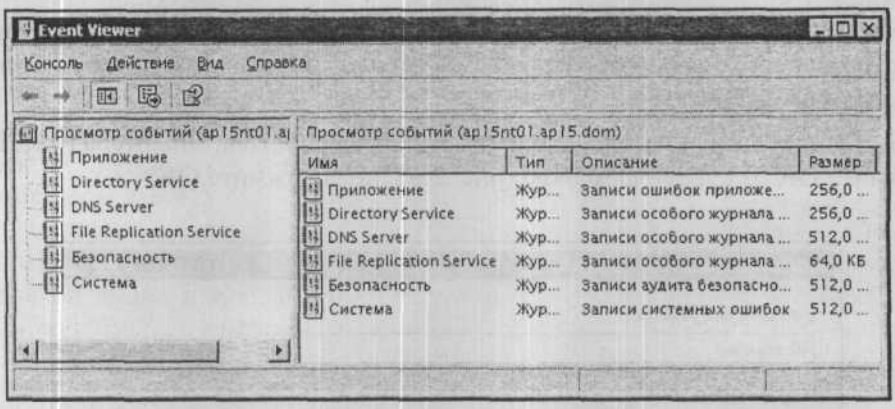

Рис. 2.7. Окно просмотра событий сервера

Вы можете просматривать записи из любого журнала на сервере (рис. 2.8).

Теперь представьте себе ситуацию, когда для решения какой-либо проблемы в сети вам необходимо просмотреть журналы событий не только на сервере, но и на нескольких рабочих станциях, которые территориально удалены от вас на десятки метров. Подключаясь к компьютерам описанным способом, вы можете за короткое время получить значительный объем информации, не только не подходя к серверу и рабочим станциям, но и не беспокоя пользователей, продолжающих в это время работать в обычном режиме.

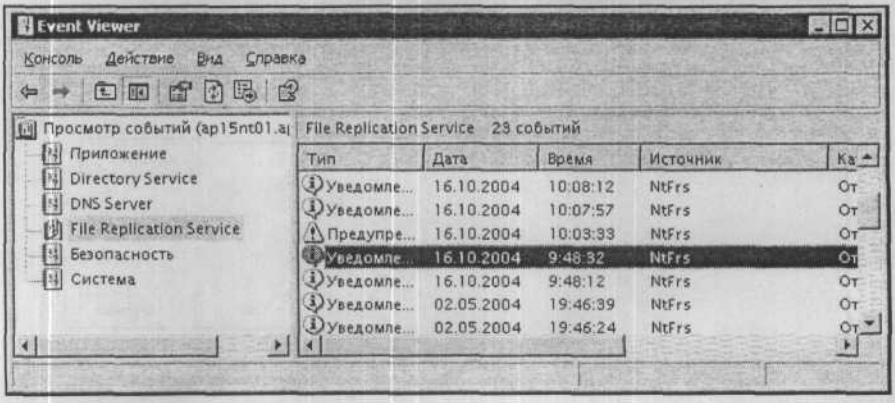

Рис. 2.8. Окно просмотра событий сервера с открытым журналом службы репликации файлов (**File Replication Service**)

Из командной строки

Теперь посмотрите на рис. 2.3. В верхней трети этого окна можно увидеть надпись "Тип: Ошибка Код(ID): 15". Каждое сообщение в журналах событий имеет свой тип и код-идентификатор (ID). Каждому идентификатору соответствует определенное описание события. Просматривая журналы событий, вы можете обратить внимание на периодическое появление какой-либо ошибки или другого события, которое вас заинтересовало. Просмотреть все сообщения даже в одном журнале — работа не из приятных. Количество записей в журнале достаточно велико, и чтобы найти записи одного вида, придется потратить достаточно много времени. Но Windows XP содержит в своем составе утилиту, написанную на VBScript, которая позволяет отфильтровать записи журналов по определенным критериям, определив дату и время появления сообщения о событии. После этого намного легче найти все интересующие сообщения, чтобы определить связь между их появлением и событиями, происходящими в сети или в системе компьютера. Эта утилита называется eventquery.vbs. Для ее запуска необходимо выполнить `cmd`, а затем в командной строке ввести следующее:

```
cscript c:\windows\system32\ eventquery.vbs /<параметры>.
```

В качестве параметров допустимы следующие значения:

- `/l` <"имя_журнала_по_английски"> — определяет журнал, в котором ведется поиск;
- `/s` — все сообщения;
- `/r N` — N последних событий;
- `/r -N` — N самых старых событий;
- `/r N-M` — события от N до M;
- `/fi "id eq XXX"` — все сообщения с идентификатором XXX;
- `/fi "id nq XXX"` — все сообщения с идентификатором не равном XXX;
- `/fi "id ge XXX"` — все сообщения с идентификатором большим или равным XXX;
- `/fi "id lt XXX"` — все сообщения с идентификатором меньшим XXX;
- в строке параметров можно применить оператор `or` — или выражение `/fi "id eq YYY or id eq ZZZ" /r 20` — все события с номерами YYY или ZZZ.

Параметры, начинающиеся на `/fi` (фильтры), можно комбинировать.

Для доступа к серверу из сети следует добавить параметры `/s systemname`, `/u username` и `/p password`, где `systemname` — имя сервера, `username` — имя пользователя, `password` — пароль доступа.

Для вывода информации в файл с разделителями в виде запятых следует добавить параметр `/fo csv`.

Чтобы информация действительно выводилась в файл, как обычно в командной строке следует после команды поставить знак ">" и написать имя файла с указанием полного пути к нему. Все имена и пути, содержащие пробелы, следует заключать в кавычки.

Кроме идентификатора ID, можно фильтровать сообщения по дате и времени — datetime, типу — type, пользователю — user, компьютеру — computer, источнику сообщения — source, категории сообщения — category.

На рис. 2.9 показано окно командной строки с выполненной командой

```
cscript c:\windows\system32\ eventquery.vbs /l application /fi "datetime
ge 11/24/04,05:00:00PM"
```

Эта команда вывела на экран все сообщения локального журнала приложений после 24 ноября 2004 года 17 часов 00 минут 00 секунд на момент выполнения, равный 24 ноября 2004 года 20 часов 15 минут 00 секунд.

Добавив к строке команды

```
/fo csv > c:\err.csv,
```

вы получите результат выполнения команды в файле err.csv на диске C:. Файл будет записан в DOS-кодировке.

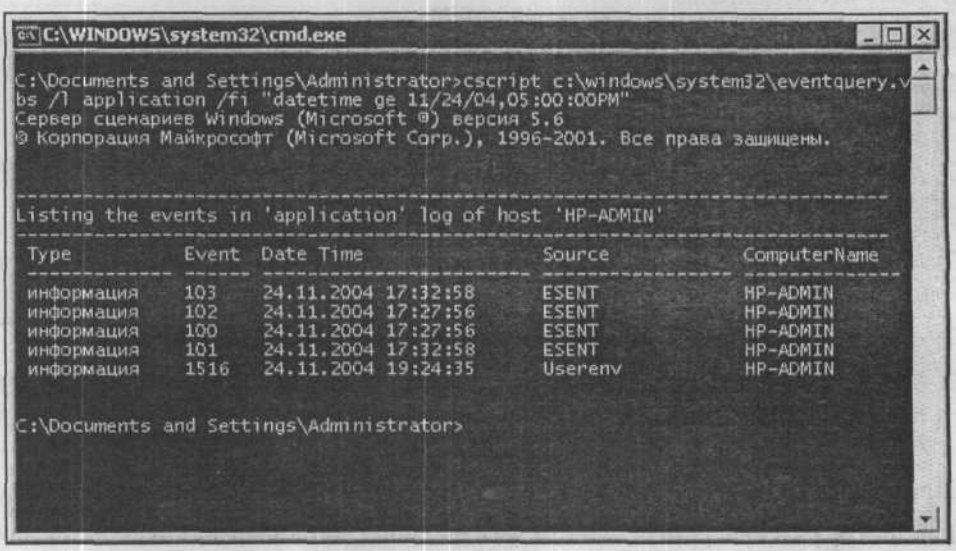

Рис. 2.9. Окно командной строки с выполненной командой `eventquery`

Не очень удобно вводить вручную такие длинные команды. Но существуют пакетные и командные файлы, в которых эти команды можно записать заранее и выполнять по мере необходимости. Если команда записана неправильно, то вы увидите на экране сообщение об ошибке и, возможно, рекомендацию, как следует написать команду. Дополнительную информацию о работе утилиты eventquery.vbs можно почерпнуть, открыв этот файл в текстовом редакторе и проанализировав его код.

Не знаю, как вам, а мне эта утилита понравилась уже при первом знакомстве с ней.

Сообщения об ошибках (две утилиты)

С различными сообщениями об ошибках вы можете встретиться не только в журналах событий. Это могут быть сообщения ОС во время установки программ, сообщения, связанные со сбоями в работе программ, ошибки доступа к различным ресурсам, и т. д. Невозможно перечислить все случаи возникновения сообщений об ошибках и привести их описания. Иногда сообщения системы могут поставить в тупик даже очень опытного пользователя. Для того чтобы разобраться в ситуации, можно применить утилиты, которые позволяют "расшифровать" непонятные сообщения системы. К сожалению, этих утилит нет в самой ОС, их придется скачать из Интернета. Утилиты бесплатны.

Exchange Server Error Code Look-up

Первая утилита работает из командной строки и называется Exchange Server Error Code Look-up (просмотр кодов ошибок сервера Exchange), имя файла — err.exe. Пусть вас не пугает, что в названии утилиты упоминается "Exchange Server". Вероятно, при работе с сервером обмена информацией необходимость поиска источника ошибки велика, а определение этого источника без вспомогательных средств затруднительно. Утилита работает и просто в операционной системе Windows XP/2000/2003. Известно, что сообщения об ошибках, возникающих при выполнении программ, выводятся только потому, что программисты предусмотрели вывод таких сообщений. Если известен код ошибки, то должно быть и ее соответствующее описание. Правда, в разных операционных системах некоторые одинаковые ошибки могут иметь различные коды. Так вот, чтобы именно в вашей системе найти возможно больше информации о конкретной ошибке, удобно применить эту утилиту. Найти ее можно по адресу в Интернете:

www.microsoft.com/downloads/details.aspx?familyid=
be596899-7bb8-4208-b7fc-09e02a13696c&displaylang=en.

Использование:

```
err <значение> [значение] [значение] ...
```

где <значение> должно иметь одну из следующих форм:

- шестнадцатеричное (0x54f);
- *неявное шестнадцатеричное* (54f);
- неоднозначное (1359) — программа будет искать значения 0x1359 и 1359;
- точная строка сообщения об ошибке (=ERROR_INTERNAL_ERROR);
- подстрока (:INTERNAL_ERROR).

Программа ищет всю информацию об ошибке в так называемых заголовочных файлах системы с расширением *.h (C:\WINDOWS\system32\).

Далее приведен пример выполнения `err 0x5dc`, что соответствует поиску ошибки с кодом 1500. На экран будет выведена следующая информация:

```
# for hex 0x5dc / decimal 1500 :
ecScottBriggsMin                ec.h
SCEEVENT_INFO_BACKUP_SECURITY          uevents.mc
# Security configuration was backed up to %1.
ERROR_EVENTLOG_FILE_CORRUPT          winerror.h
# The event log file is corrupted.
# 3 matches found for "0x5dc"
```

Пример был выбран случайным образом и не связан с конкретной ситуацией в системе, тем не менее видно, что появление такой ошибки может быть вызвано разрушением лог-файла событий (`The event log file is corrupted`), например.

Error Messages for Windows

Эта утилита выполняется в обычном окне Windows. Найти ее можно по адресу в Интернете:

http://www.gregorybraun.com/MSWinErr.html.

Данная утилита использует информацию из библиотеки Shellapi.dll, что заставляет ее разговаривать с вами на языке вашей системы. Об этой программе можно почти ничего не рассказывать, достаточно посмотреть на два скриншота (рис. 2.10, 2.11), и вам все станет понятно.

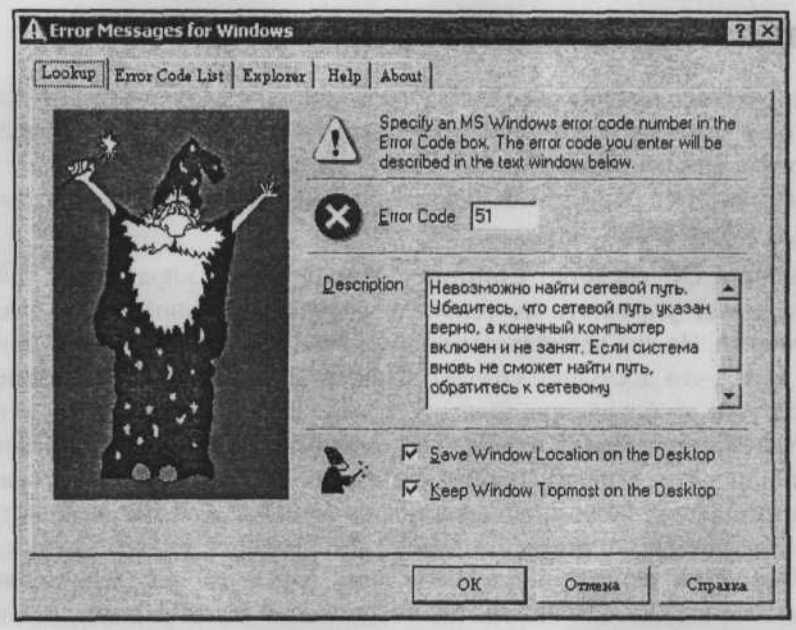

Рис. 2.10. Окно **Error Messages for Windows** с информацией о конкретной ошибке

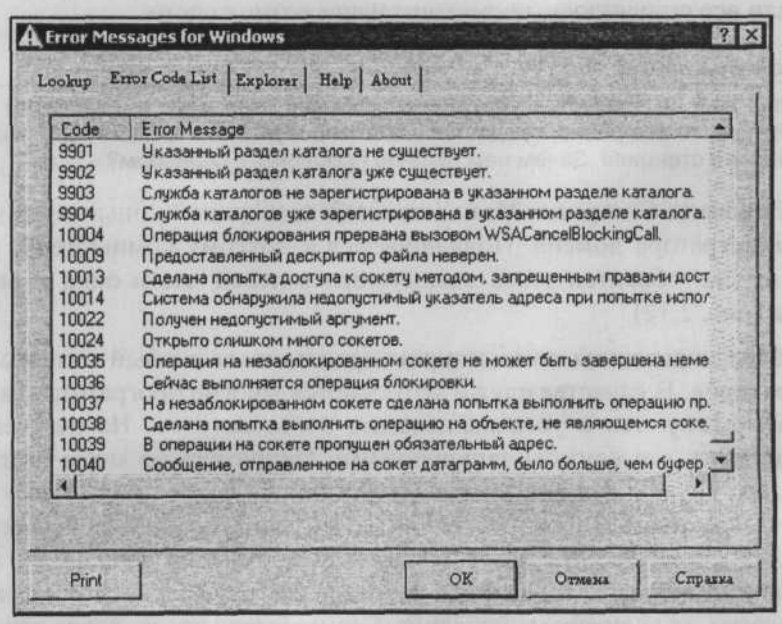

Рис. 2.11. Окно **Error Messages for Windows** с перечнем описаний ошибок, доступных в системе

Управление компьютером

Надеюсь, что управление своей рабочей станцией у вас проблем не вызывает, а если они возникают, то решаются самостоятельно. Здесь мы рассмотрим некоторые средства управления удаленными системами, к которым главным образом относится сервер. Возможно применение этих средств и для управления удаленными рабочими станциями.

Встроенное в ОС средство **Computer Management** (Управление компьютером) позволяет управлять не только локальной машиной, но и удаленным компьютером. Не все возможности локального управления можно применить в сети, но то, что доступно, создает значительные удобства для администратора. Для того чтобы воспользоваться этими удобствами, достаточно открыть **Computer Management** (Управление компьютером) от имени администратора домена, а затем в меню **Действие** выбрать опцию **Подключиться к другому компьютеру**. Если процедура подключения к другому компьютеру вызывает затруднения, то просмотрите еще раз описание подключения к журналам событий на сервере в начале главы. Если вы все делаете верно, а подключение не удается, то возможно, что вы не входите в число администраторов удаленного компьютера. Придется в этом случае дойти до рабочей станции и настроить для себя (администратора домена) права ее администратора. Если все получилось, посмотрим наши возможности.

Замечание

Если вам не требуется управление рабочей станцией, а необходим доступ к серверу, то все равно, предварительно опробуйте это средство для управления рабочей станцией. Зачем вам лишние проблемы с сервером?

Итак, открываем **Computer Management** (Управление компьютером) от имени администратора домена. Подключаемся к другому компьютеру, разворачиваем дерево объектов этого компьютера в левой части окна и выбираем **Службы** (рис. 2.12).

Этот раздел управления компьютером представляет особый интерес для администраторов. В качестве служб запускаются многие программы, как встроенные в систему, так и устанавливаемые пользователем. Но не всегда есть смысл держать все службы запущенными. Например, на моем компьютере установлена служба факсов, но используется она так редко, поэтому обычно находится в остановленном состоянии, а это экономит ресурсы компьютера при повседневной работе. Многим известна программа удаленного администрирования Radmin, которая тоже работает как служба. Администратор может запускать эту службу на удаленном компьютере тогда, когда это необходимо, экономя ресурсы удаленной рабочей станции и повышая ее защищенность от несанкционированного доступа.

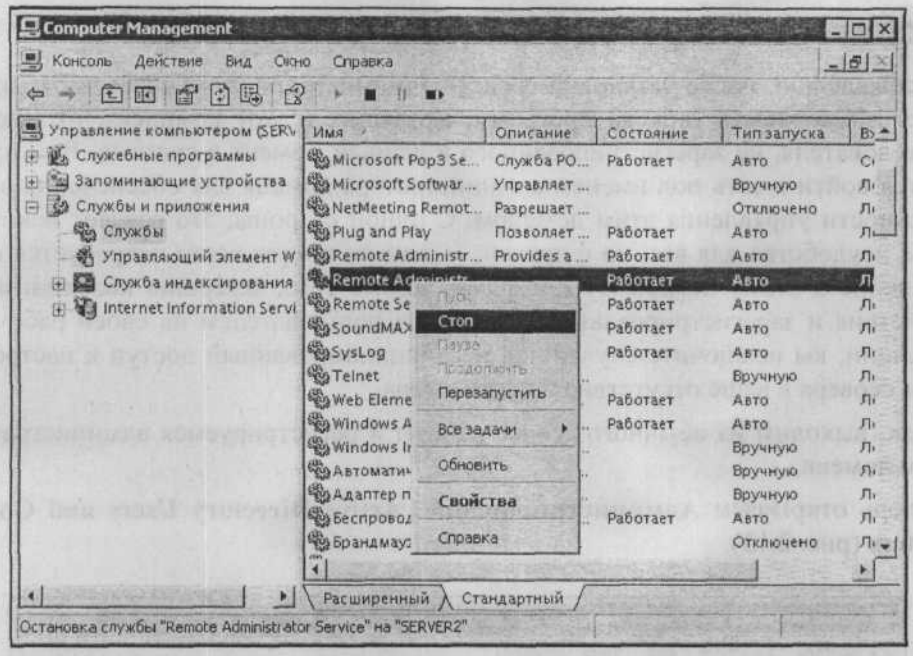

Рис. 2.12. Окно **Computer Management** с открытым контекстным меню службы

Как и в случае локального доступа, вы можете запускать и останавливать службы, выполнять любые другие действия с ними, доступные при локальном доступе.

Аналогично можно управлять и учетными записями пользователей на удаленном компьютере, используя опцию **Служебные программы** в окне **Computer Management** (Управление компьютером). Но в нашей сети локальные пользователи есть только на втором сервере. Основной сервер настроен на применение службы каталогов Active Directory. В этом случае невозможно получить доступ к учетным записям пользователей в AD с локальной машины без дополнительных средств. Такие средства можно найти на дистрибутивных дисках серверных операционных систем. В каталоге i386 дистрибутивного диска найдите файл adminpak.msi и запустите установку этого средства на вашем компьютере. После его установки в папке **Администрирование** появится несколько новых ярлыков, включая **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).

Примечание

Важно учесть, что установка этого средства будет возможна при совпадении языка вашей операционной системы и системы на дистрибутивном диске. Если вы используете английскую версию Windows XP, то и дистрибутив серверной операционной системы должен быть английской версии. При этом все наименования объектов будут английскими.

Active Directory — удаленное управление

К сожалению, после установки средств администрирования сервера отсутствует возможность запуска программ, входящих в этот комплект, от имени пользователя, не зарегистрированного в данный момент в системе. Вам придется войти в сеть под именем администратора домена для обеспечения возможности управления этим доменом. С одной стороны, это создает некоторые неудобства для вас, но с другой, — вам не так уж часто потребуется обращение к этому комплекту программ. Кроме того, завершив необходимые действия и зарегистрировавшись обычным пользователем на своей рабочей станции, вы исключите случайный несанкционированный доступ к настройкам сервера в ваше отсутствие у компьютера.

Итак, выходим из обычного сеанса работы и регистрируемся администратором домена...

Теперь открываем **Администрирование | Active Directory Users and Computers** (рис. 2.13).

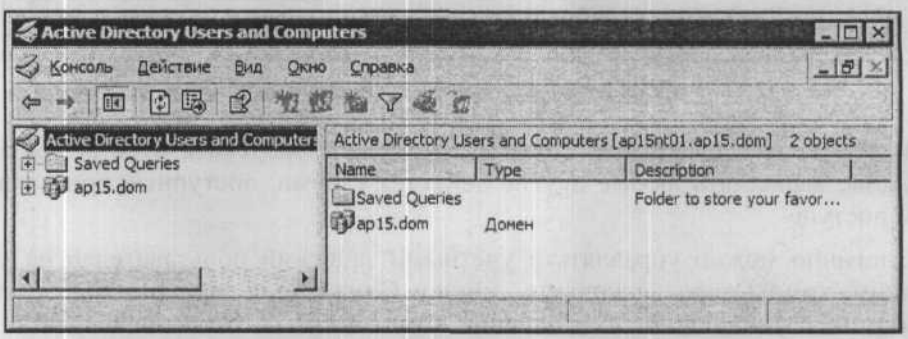

Рис. 2.13. Окно **Active Directory Users and Computers**

Если вы не увидели значка своего домена в правой части окна, то следует выполнить следующие действия:

1. Нажмите кнопку **Действие.**
2. Выберите **Connect to Domain** (Подключиться к домену).
3. Впишите имя вашего домена в доступное для этого поле.
4. Отметьте **Save this domain setting for the current console** (Сохранить настройки для текущей консоли).
5. Нажмите **OK**.

После этого при входе в консоль управления службой каталогов Active Directory подключение будет осуществляться автоматически.

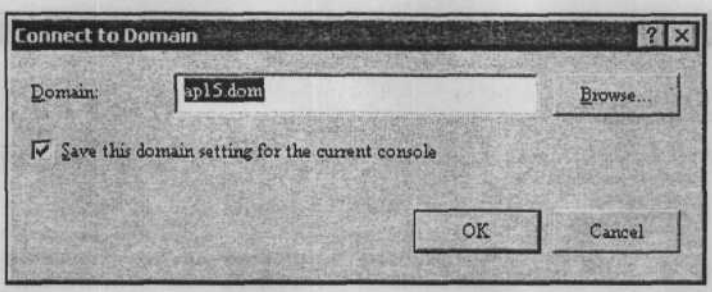

Рис. 2.14. Окно **Connect to Domain**

Развернув объект с именем вашего домена, вы получите доступ ко всем подразделениям, пользователям и компьютерам, зарегистрированным в домене. Все действия, которые доступны при локальном доступе к серверу, доступны и из этого окна (рис. 2.15).

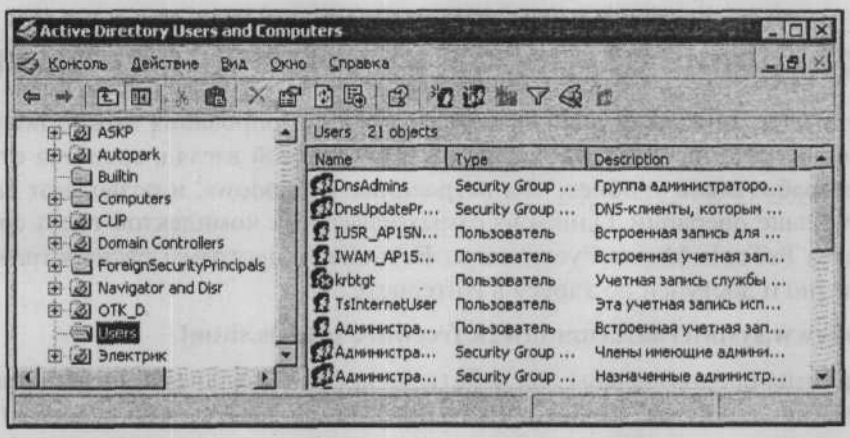

Рис. 2.15. Окно **Active Directory Users and Computers** с развернутой структурой домена

Сервер DHCP

В *главе 1* мы уже рассматривали настройку этого сервера.

Здесь лишь приведем вид окна этого сервера при доступе из сети (рис. 2.16).

С помощью пакета административных программ вы можете управлять всеми компонентами службы каталогов Active Directory, работающими на вашем сервере, не сходя со своего рабочего места.

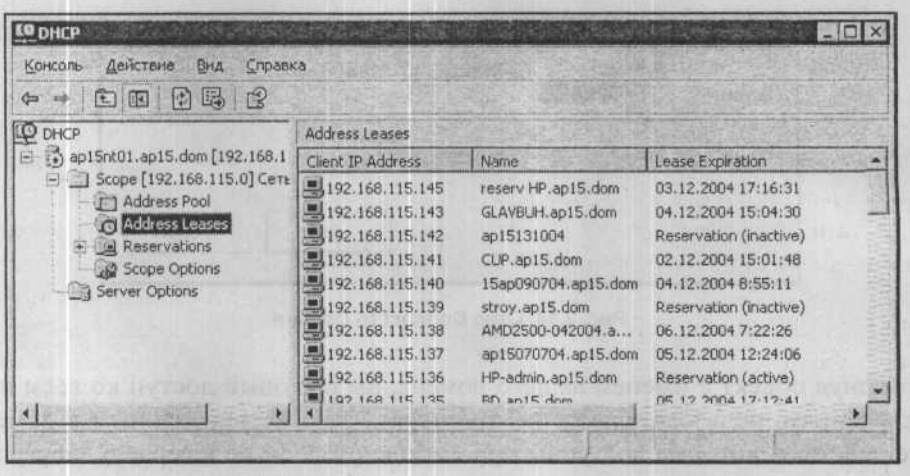

Рис. 2.16. Окно DHCP при доступе с рабочей станции

Управление сервером из командной строки

Полезные возможности для удаленного администрирования можно получить применяя средства командной строки. Пока, на мой взгляд, средства сторонних разработчиков удобнее, чем встроенные в Windows, и позволяют выполнять больше операций. Одним из самых известных комплектов таких средств является PsTools Марка Русиновича. Весь пакет программ распространяется бесплатно и доступен по адресу в Интернете:

http://www.sysinternals.com/ntw2k/freeware/pstools.shtml.

Программы предназначены для работы со всеми серверными операционными системами семейства Windows. Ряд утилит командной строки содержит сама операционная система.

Надо сказать, что с появлением графического интерфейса многие пользователи стали избегать командной строки, как менее понятного, чем программы с графическим интерфейсом, средства. Графический интерфейс часто понятен интуитивно, назначение кнопок указано явно, и нам остается выбрать предполагаемое действие. Если что-либо не понятно, есть средства справочной системы Windows, где чаще всего можно найти пояснения к работе с программами, входящими в состав ОС. Командная строка многих пугает своей чернотой и "неизвестностью". Тем не менее средства командной строки во многих случаях оказываются полезнее программ с графическим интерфейсом. Даже при обычной локальной работе на компьютере есть ситуации, когда ничто, кроме командной строки, вам не поможет. Так, например, если Windows не загружается в обычном режиме, вы можете загрузиться в режиме

командной строки или запустить консоль восстановления. Но это крайний случай, когда система не работоспособна. Бывает и так, что все работает, но требуется выполнить действие, которое невозможно выполнить обычными средствами Windows. Однажды моя ошибка привела к появлению в системе 6500 копий файлов с именами, отличающимися от оригиналов символами (2) в конце имени. Система продолжала работать, но файлы занимали очень много места и просто раздражали своим присутствием. Расположены они были в различных каталогах пользователей и системы, что не позволяло их быстро удалить обычными средствами. Я попытался применить средство поиска файлов, а затем удалить файлы прямо из окна поиска. Оказалось, что так можно удалить лишь небольшое количество файлов за один прием. В моем случае система не могла справиться с этой задачей. На помощь пришла команда `del` из командной строки. Указав соответствующие параметры этой команды, удалось за несколько секунд очистить систему от мусора. Кому интересно, привожу вид команды:

```
del /s /q c:\ *(2).*.
```

Возможно, что у вас возникла мысль: "А зачем здесь информация о локальной работе в системе?" На это отвечу следующее: возможности удаленного администрирования практически безграничны. Даже локально применяемые команды могут пригодиться, когда вы их сможете применить на удаленной машине.

Рассмотрим некоторые из программ комплекта PsTools и пакета Support Tools (Resource KIT), находящиеся на дистрибутивных дисках ОС.

Remote.exe (Support Tools)

В пакетах Support Tools серверных операционных систем есть утилита remote.exe, которая позволяет выполнить задачу управления из командной строки. Эта утилита требует своего запуска на сервере, а затем на рабочей станции, с которой предполагается управление. Скопировав remote.exe в любой каталог на сервере, следует в командной строке, войдя в каталог с утилитой, набрать

```
remote /s "cmd" /v,
```

где `s` — команда запуска серверной части remote, `"cmd"` — командная строка, `v` — программа запускается в видимом режиме.

На рабочей станции требуется в командной строке ввести

```
remote /c <имя_сервера> /v
```

Параметр `/c` говорит о запуске клиентской части программы. Через несколько мгновений мы окажемся в каталоге, из которого на сервере была запущена

утилита. Теперь можно выполнять любые команды из командной строки. Можно создавать и удалять каталоги или копировать файлы, выполнять команду `ipconfig` для просмотра конфигурации IP-протокола на сервере и многое другое.

Единственное, что несколько омрачает удовольствие от применения этой утилиты, так это то, что она не воспроизводит русских шрифтов, выводимых программами на экран, но русские имена каталогов и файлов поддерживаются вполне корректно. Выполнения некоторых команд вы не увидите. Например, попытка вывести на экран содержания текстового файла (`copy file.txt con`) приведет к тому, что результат будет виден на сервере, а на вашем экране появится только сообщение о выполненной команде. Но команда `type file.txt` будет выполнена как положено, при этом русский текст будет читаться, если он в DOS-кодировке. Все команды, выполняемые с рабочей станции, на сервере сопровождаются пометками, сообщающими, с какой рабочей станции и в какое время была выполнена команда. Попытка запуска программы с графическим интерфейсом приводит к невозможности дальнейшего ввода команд и необходимости закрытия окна командной строки на сервере.

Для того чтобы закрыть сеанс связи с сервером в нормальном режиме, следует набрать команду `@K`.

Словом, утилита remote.exe вполне может стать вашим помощником при администрировании сервера.

PsExec (PsTools)

Эта утилита упоминается здесь, поскольку, читая ее оригинальное описание, вам очень захочется ее испытать. Но результат может не оправдать ожидания.

В описании, прилагаемом к комплекту программ, сказано, что утилита PsExec позволяет выполнять на удаленном компьютере программы командной строки. К сожалению, мне не удалось воспользоваться этой программой. В результате попыток ее применения на удаленных компьютерах устанавливалась служба, которая должна была обеспечить связь с сервером удаленной машины. Вероятно, последние обновления безопасности для Windows запретили этой службе выполнять свои функции. Пришлось воспользоваться программой srvinstw.exe для удаления следов PsExec на сервере. Эта утилита помогает удалить службу, если она не нужна, но вручную ее удалить не удается. Найти srvinstw.exe можно по адресу **http://www.softodrom.ru/win/p83.shtml**.

PsInfo (PsTools)

Эта утилита позволяет собрать сведения об удаленной системе.

Использование:

```
psinfo [\\компьютер [,компьютер [...] | @file [-u имя_пользователя
[-p пароль]]] [-h] [-s] [-d] [-c]
```

где:

\\ компьютер — имя компьютера, о котором необходимо получить сведения. Если указать *, тогда команда выполняется для всех компьютеров в текущем домене;

@file — файл с перечнем компьютеров, о которых необходимо получить сведения;

-u — определяет имя пользователя для входа в систему на удаленный компьютер;

-p — определяет пароль для имени пользователя;

-h — показать установленные обновления;

-s — показать установленное программное обеспечение;

-d — показать информацию о дисках;

-c — выводить в формате CSV (comma-separated value, значения, разделяемые запятой).

PsList (PsTools)

Эта утилита позволяет получить сведения о процессах на удаленном компьютере, использовании памяти, выводя статистику в непрерывном режиме (можно указать период обновления информации в секундах).

Использование:

```
pslist [-d] [-m] [-x][-t][-s [n] [-r n] [\\компьютер
[-u имя_пользователя] [-p пароль]] [[-e] имя_процесса | идентификатор
процесса]
```

где:

-d — показать статистику для всех активных потоков;

-m — информация об использовании памяти;

-x — использование памяти каждым из процессов;

-t — показать дерево процессов;

-s [n] — выполнять программу через n секунд;

`-r n` — возобновить работу после окончания;

`-u` — имя пользователя для входа в систему на удаленный компьютер;

`-p` — пароль для имени пользователя.

PsKill (PsTools)

Это средство уничтожения процессов на удаленной машине.

Использование:

```
pskill [\\компьютер [-u имя_пользователя] [-p пароль]] <имя_процесса |
идентификатор_процесса>
```

Для двух последних утилит есть похожие в составе Support Tools, это Tlist.exe и kill.exe. Но это не полные аналоги, поскольку работают только локально.

PsLoggedOn (PsTools)

Эта утилита позволяет увидеть имена учетных записей пользователей, подключенных в данный момент к серверу.

Использование:

```
psloggedon [-l] [-x] [\\компьютер]
```

где:

`-l` — показать только локальных пользователей;

`-x` — не показывать время подключения.

> ***Примечание***
>
> Для большей комфортности работы с командной строкой все утилиты лучше поместить в один каталог. В свойствах ярлыка командной строки нужно указать в качестве рабочего каталога именно эту папку с полным путем к ней (поле **Рабочая папка** на вкладке **Ярлык** в окне свойств ярлыка).

Качество работы сети

Утилиты, рассмотренные выше, позволяют получить информацию об удаленной машине и выполнить на ней некоторые действия. Но администратору необходимо следить за качеством работы сети в целом. Качество работы сети определяется качеством связи между компьютерами, а также отсутствием лишних доступных ресурсов в ней. Для контроля над работой сети также существуют соответствующие программы и утилиты.

Ping

Одна из самых простых в использовании программ — C:\ windows\ system32\ ping.exe. Благодаря размещению программы в системной папке, путь к которой определен в конфигурации системы, запускать ее можно, находясь в любом каталоге компьютера. Эта команда присутствует во всех операционных системах, поддерживающих работу в сети. Особенности команды, список ее параметров может отличаться от системы к системе, но основные функции неизменны. Ниже приведен результат применения команды ping, который можно увидеть на экране компьютера в окне командной строки (сеанс DOS) или в режиме DOS:

```
Ping 192.198.0.142

Обмен пакетами с 192.168.0.142 по 32 байт:

Ответ от 192.168.0.142: число байт=32 время<10мс TTL=128
Ответ от 192.168.0.142: число байт=32 время<10мс TTL=128
Ответ от 192.168.0.142: число байт=32 время<10мс TTL=128
Ответ от 192.168.0.142: число байт=32 время<10мс TTL=128

Статистика Ping для 192.168.0.142:
    Пакетов: послано = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время передачи и приема:
    наименьшее = 0 мс, наибольшее =  0 мс, среднее =  0 мс
```

Команда позволяет определить следующие параметры сети:

- доступность компьютера в сети;
- работоспособность кабельной линии (линий) между вашим и удаленным компьютером;
- качество связи между компьютерами.

Проложив новую кабельную линию и увидев, что время прохождения пакета более 1 мс, можно сделать вывод о том, что линия проложена плохо. Возможно, что рядом оказались провода высокого напряжения или категория кабеля ниже необходимой. Заменяя обычный хаб (концентратор) на коммутатор, который поддерживает скорость передачи данных 100 Мбит/с, вы можете обнаружить ухудшение связи между компьютерами. Причин может быть несколько, но перенастроив порты коммутатора на пониженную скорость, вы восстановите нормальную связь.

Ipconfig

Эта команда тоже запускается из командной строки. Она позволяет определить сетевые настройки компьютера, на котором она запущена. Ниже приве-

ден пример ее выполнения с параметром all, доступным в операционных системах Windows:

```
Ipconfig /all

Настройка IP для Windows 98
        Главный компьютер . . . . . : Prog.AP15.dom
        Серверы DNS . . . . . : 192.168.0.15
        Тип узла  . . . . . : Гибридный
        Код области NetBIOS ID  . . . . . :
        Переадресация IP. . . . . : Нет
        Включение WINS Proxy. . . . . : Нет
        Разрешение NetBIOS через DNS . . .  : Да

0 Ethernet: плата :
        Описание. . . . . : PPP Adapter.
        Физический адрес. . . . . : 44-45-53-54-00-00
        Включение DHCP. . . . . : Да
        IP-адрес. . . . . : 0.0.0.0
        Маска подсети . . . . . : 0.0.0.0
        Стандартный шлюз. . . . . :
        Сервер DHCP . . . . . : 255.255.255.255
        Первичный сервер WINS . . . . . :
        Вторичный сервер WINS . . . . . :
        Доступ получен. . . . . :
        Доступ истекает . . . . . :

1 Ethernet: плата :
        Описание. . . . . : Compex RE100TX PCI Fast
                                Ethernet Adapter
        Физический адрес. . . . . : 00-40-95-30-95-64
        Включение DHCP. . . . . : Да
        IP-адрес. . . . . : 192.168.0.101
        Маска подсети . . . . . : 255.255.255.0
        Стандартный шлюз. . . . . :
        Сервер DHCP . . . . . : 192.168.0.15
        Первичный сервер WINS . . . . . : 192.168.0.15
        Вторичный сервер WINS . . . . . :
        Доступ получен. . . . . : 22/06/03 09:27:13
        Доступ истекает . . . . . : 30/06/03 09:27:13
```

Без параметров эта команда покажет только сведения об IP-адресах. При неполадках, которые могут быть вызваны неправильными настройками рабочей станции, вы можете проверить эти настройки, пользуясь описанной коман-

дой. Имея средства для выполнения программ командной строки на удаленном компьютере, эту команду можно применять и для контроля настроек удаленных рабочих станций или сервера.

SuperScan — программа для сканирования сетей

Большую помощь может оказать бесплатная утилита SuperScan (рис. 2.17), которую можно найти по адресу:

http://www.snapfiles.com/get/superscan.html.

Эта утилита позволяет определить активные в данный момент компьютеры в сети. Сеть сканируется в заранее заданном диапазоне адресов и портов. Поскольку в вашей сети большинство адресов не выходит за пределы заранее определенных значений, найти активные машины не составит труда. Программа позволяет определить IP-адреса, имена компьютеров, открытые порты на каждой машине. При необходимости определить доступность компьютеров в сети, вы получите полную картину ситуации, запустив эту программу.

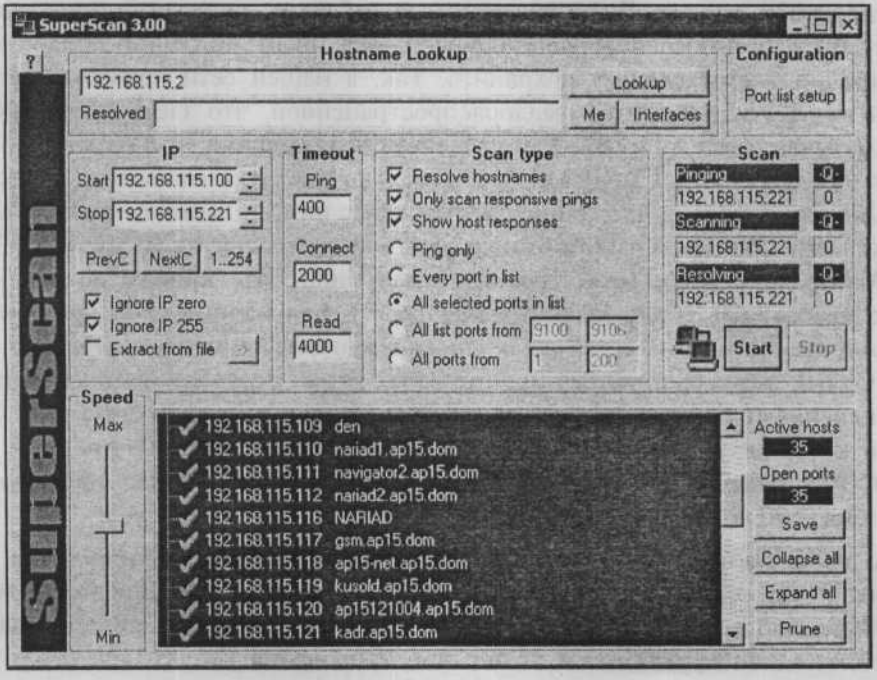

Рис. 2.17. Утилита SuperScan 3.00

Эта утилита удобна и при сборе статистики о работе компьютеров в сети. Результат работы программы может быть сохранен в файле. Запуская програм-

му в определенные часы и сохраняя результат сканирования, вы получите достоверные сведения о работе компьютеров в эти часы. На каждом компьютере, просканированном программой, можно определить открытые порты, что может потребоваться при выяснении причин неработоспособности программ, требующих для нормальной работы открытия конкретных портов.

Существует более новая версия этой программы (4.0), но в ней очень много отличий и в интерфейсе, и в удобстве работы, причем, на мой взгляд, не в лучшую сторону. В нашей сети продолжает применяться версия, описанная здесь.

Автоматизация обслуживания базы данных

Этот вопрос в каждой сети ставится и решается по-своему. Но, учитывая широкое распространение СУБД MS Access различных версий, рассмотрим работу с такой базой в сети, где несколько пользователей регулярно обращаются к ней в процессе работы. При этом требуется решать обычные сетевые задачи: резервное копирование базы данных, сжатие базы данных, обеспечение безопасности данных. Возможно, что для работы с другими базами данных набор средств для обслуживания должен быть иным, но общий подход к решению проблемы следует сохранить. Так, в нашей сети применяется еще один вид СУБД, настолько малораспространенной, что здесь мы не будем рассматривать работу с ней. Тем не менее обслуживание этой базы отличается от обслуживания СУБД MS Access только инструментальными средствами. Любое сетевое приложение, работающее с базами данных, имеет клиентскую часть, с которой работают пользователи, и серверную. В случае с СУБД MSAccess, на сервере может располагаться лишь база данных, но для большего удобства ее обслуживания на сервере установлено и само приложение MS Access. Во многих сетях небольшого масштаба применяется именно этот вид СУБД, позволяющий без значительных затрат разрабатывать клиентские приложения и при необходимости быстро модернизировать структуру базы данных. По ряду причин, несмотря на наличие лицензионного дистрибутива MS Office более поздних версий, для работы в сети у нас применяется MS Access 97.

Базы данных в нашей сети предназначены для решения различных задач. Тем не менее по некоторым видам данных они пересекаются. Для исключения двойного ввода одних и тех же данных осуществляется их синхронизация. Это тоже одна из рутинных задач администрирования.

Для упрощения работы администратора практически все задачи по обслуживанию баз данных автоматизированы. Именно такой автоматизированный вариант обслуживания и будет рассмотрен далее.

Для наглядности описания процедур по обслуживанию базы данных все элементы системы обслуживания изобразим на рис. 2.18.

Все данные (**Первая база данных** и **Вторая база данных**) находятся на главном сервере. Резервные копии данных создаются на вспомогательном сервере. Для бесперебойного функционирования всей системы необходимо производить обмен данными между двумя базами данных, а также выполнять сжатие баз данных.

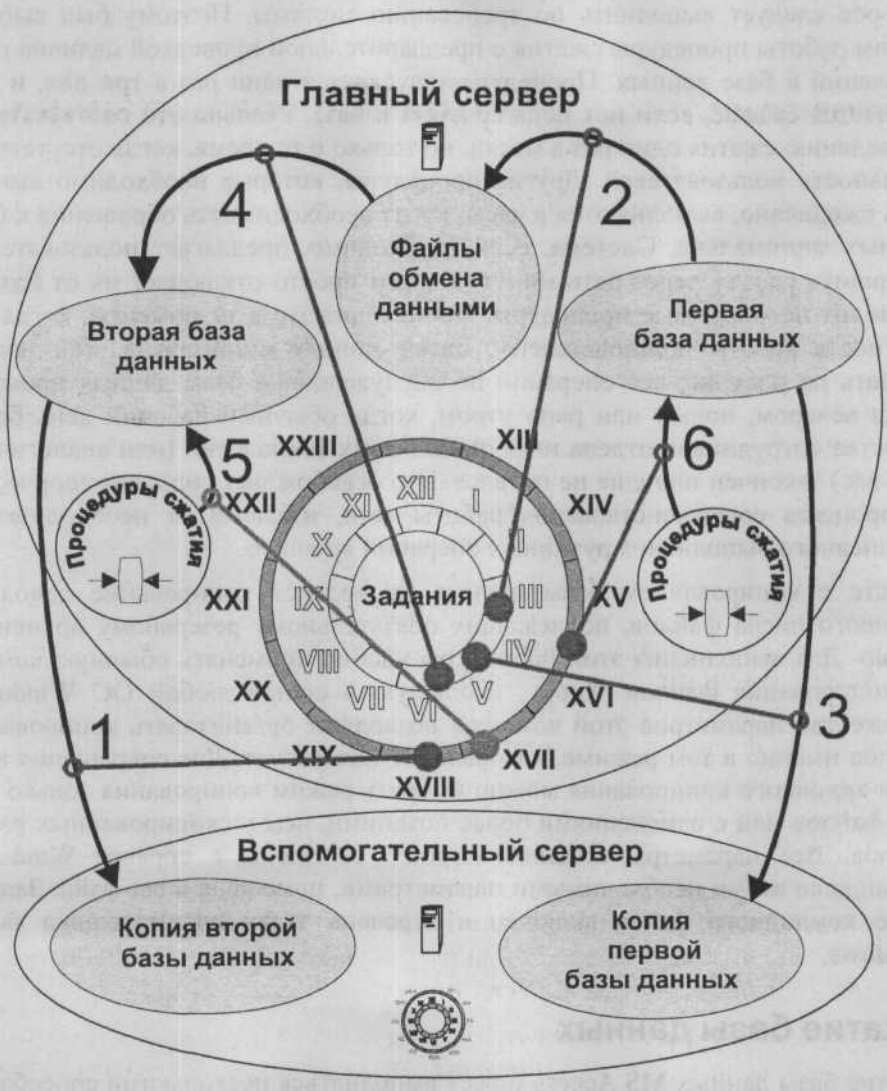

Рис. 2.18. Автоматизация обслуживания баз данных в сети

Все перечисленные задачи выполняются автоматически без вмешательства администратора по заранее составленному графику. Выполнение графика обслуживания осуществляется стандартным планировщиком заданий, имеющимся в ОС. Время для выполнения отдельных операций выбиралось исходя из режима работы пользователей с системой. Процедура сжатия базы данных не требует ежедневного выполнения. Время, необходимое на осуществление этой операции, невелико, но при активной работе пользователей может раздражать, если ее проводить ежедневно, необходимость отключения от базы, которое следует выполнить по требованию системы. Поэтому был выбран режим работы процедуры сжатия с предварительной проверкой наличия подключений к базе данных. Процедура запускается один раз в три дня, и выполняется сжатие, если нет подключений к базе. Реально это соответствует проведению сжатия один раз в месяц, но только в то время, когда отсутствует активность пользователей. Другие процедуры, которые необходимо выполнять ежедневно, выполняются в часы, когда необходимость обращения к базе данных минимальна. Система, если необходимо, предлагает пользователям завершить работу через пять минут, а затем просто отключает их от базы и проводит необходимые процедуры. Происходит это в те моменты, когда вероятность работы пользователей с базой данных минимальна. Как можно увидеть на рисунке, все операции по обслуживанию базы данных производятся вечером, ночью или рано утром, когда обычный рабочий день большинства сотрудников отдела информационных технологий (или аналогичного у вас) закончен или еще не начался. Это освобождает силы для творческого процесса совершенствования работы сети, избавляя от необходимости ежедневного выполнения рутинных операций вручную.

Вместе с копированием базы данных проводится копирование довольно большого числа файлов, подлежащих обязательному резервному архивированию. Для выполнения этой процедуры удобно применять обычную команду копирования файлов Xcopy, входящую в состав любой ОС Windows. Множество параметров этой команды позволяют организовать копирование файлов именно в том режиме, который вас интересует. Для сокращения времени архивного копирования можно выбрать режим копирования только новых файлов или с изменениями более поздними, чем у скопированных ранее файлов. Все параметры команды хорошо освещены в справке Windows. Команда со всеми необходимыми параметрами, помещена в bat-файл. Запуск этого командного файла включен в перечень задач планировщика задач Windows.

Сжатие базы данных

Сжатие базы данных MS Access может выполняться несколькими способами, но в нашей сети был выбран вариант с применением программы, написанной

на Visual Basic 6.0. Для работы программы в автоматическом режиме не обязательно наличие формы, появляющейся на экране. Но с целью упрощения отладки всей системы, а также для предоставления возможности наблюдения процесса работы программы без привлечения дополнительных средств, в программе предусмотрена форма. Кроме формы, проект содержит один программный модуль (см. листинг 2.2). Создав новый проект, создайте форму, соответствующую показанной на рис. 2.19.

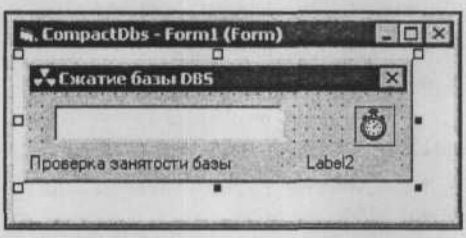

Рис. 2.19. Форма в проекте на Visual Basic

Файл формы, открытый в текстовом редакторе, будет содержать строки, приведенные в листинге 2.1. Содержания этого файла достаточно, чтобы верно повторить форму в вашем проекте.

Примечание

Если приведенный ниже материал покажется абсолютно непонятным, обратитесь к любому руководству по языку Visual Basic для освоения основных принципов программирования на этом языке. Пример готового проекта можно найти на домашней странице автора.

Листинг 2.1. Форма Form1.frm

```
VERSION 5.00
Begin VB.Form Form1
   Caption         =   "Сжатие базы DBS"
   ClientHeight    =   840
   ClientLeft      =   2535
   ClientTop       =   3360
   ClientWidth     =   3780
   Icon            =   "Form1.frx":0000
   LinkTopic       =   "Form1"
   MaxButton       =   0   'False
   MinButton       =   0   'False
   MouseIcon       =   "Form1.frx":0442
   ScaleHeight     =   840
   ScaleWidth      =   3780
```

```
   Begin VB.Timer Timer1
      Interval        =   100
      Left            =   3240
      Top             =   120
   End
   Begin VB.TextBox Поле0
      Height          =   375
      Left            =   240
      TabIndex        =   0
      Top             =   120
      Width           =   2295
   End
   Begin VB.Label Label2
      Caption         =   "Label2"
      Height          =   255
      Left            =   2760
      TabIndex        =   2
      Top             =   600
      Width           =   855
   End
   Begin VB.Label Label1
      Caption         =   "Проверка занятости базы"
      Height          =   255
      Left            =   0
      TabIndex        =   1
      Top             =   600
      Width           =   2415
   End
End
Attribute VB_Name = "Form1"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = False

Private Sub Form_Activate()
Me.Label2.Caption = Time

Модуль.compress

End
End Sub
```

Модуль, входящий в состав проекта, имеет следующее содержание, представленное в листинге 2.2. В текст модуля, приведенный в книге, добавлены комментарии, поясняющие работу программы.

Листинг 2.2. Содержание программного модуля "Модуль" проекта

```
Sub compress()

Dim db1 As Database
Dim Er1 As Label
Dim bl1 As Label
Dim bl2 As Label
Dim i As Integer
Dim s As Integer
Dim MyChar As String
Dim MyChar1 As String
Dim MyChar2 As String
Dim MyChar3 As String
Dim j As Integer
Dim k As Integer
Dim l As Integer
Dim bl As Boolean
Close #i
Close #j
Close #l
'Close #2   ' Могут пригодиться при отладке
'Close #3
'Close #4
'Form1.Поле0.Text = "<Любые символы>"
' Полю формы можно присвоить значение, при отладке, при необходимости
' работы с разными базами, при необходимости указать путь к файлам.
' В данном варианте это пустое значение.

On Error GoTo Er1
' при любой ошибке переход на метку Er1
bl = True
j = FreeFile
Open Form1.Поле0.Text & "Control.txt" For Output As j
' Открыт текстовый файл "Control.txt" для записи сведений о пользователях,
' работающих с базой на момент попытки проведения сжатия.

' Далее анализируется файл, содержащий сведения об активных
' подключениях к базе.
i = FreeFile
Open Form1.Поле0.Text & "db1.ldb" For Binary As i
```

```
    Do While Not EOF(i) ' Цикл до конца файла.
        MyChar = Input(32, #i)  ' Читает 32 символа.
        k = 1
        s = 1
            Do Until s = 0
              If MyChar = "" Then Exit Do
              If s = 0 Then Exit Do
              MyChar1 = Mid(MyChar, k, 1)
              s = Asc(MyChar1)
              k = k + 1
                 If bl = False Then GoTo bl1
                 If s = 0 Then MyChar1 = " (komp) " & Chr(13) & Chr(10)
                 If s = 0 Then bl = False
                GoTo bl2
bl1:
                If s = 0 Then MyChar1 = " (user) " & Chr(13) & Chr(10)
                If s = 0 Then bl = True
bl2:
                MyChar2 = MyChar2 & MyChar1
            Loop
        Loop
    Print #j, MyChar2    ' запись в "control.txt"
    MyChar3 = Left(MyChar2, 1)
Close #i
Close #j
    If MyChar3 <> "" Then
' Если содержание файла не нулевое, в файл "Compact.txt" записывается
'сообщение о запрещении попытки сжатия, дата и время попытки.
'
        l = FreeFile
        Open Form1.Поле0.Text & "Compact.txt" For Output As 1
        Print #1, "Сжатие не разрешено! " & Date & " " & Time
        Close #1
    End If

    If MyChar3 = "" Then

' Если содержание файла нулевое, производится сжатие,
' а в файл "Compact.txt" записывается
'сообщение о завершении сжатия, дата и время сжатия.

'сжимаем база в база1,- удаляем база, потом база1 в база, удаляем база1
        Form1.Label1.Caption = "Идет сжатие - 1"

        Form1.Refresh
```

```
        DBEngine.CompactDatabase Form1.Поле0.Text & "db1.mdb", _
        Form1.Поле0.Text & "db11.mdb"

        Form1.Label1.Caption = "Идет сжатие - 2"
        Form1.Refresh

        If Dir(Form1.Поле0.Text & "db1.mdb") <> "" Then _
        Kill Form1.Поле0.Text & "db1.mdb"

        DBEngine.CompactDatabase Form1.Поле0.Text & "db11.mdb", _
        Form1.Поле0.Text & "db1.mdb"

        Form1.Label1.Caption = "Сжатие завершено"

        Form1.Refresh

          ' Проверка наличия файла базы данных и удаление
          ' промежуточного файла
        If Dir(Form1.Поле0.Text & "db11.mdb") <> "" Then _
        Kill Form1.Поле0.Text & "db11.mdb"

        l = FreeFile
        Open Form1.Поле0.Text & "Compact.txt" For Output As l
        Print #1, "Сжатие произведено! " & Date & " " & Time
        Close #1
      End If

    'MsgBox "готово"
Exit Sub

Er1:
l = FreeFile
Open Form1.Поле0.Text & "Compact.txt" For Output As l
Print #1, "Ошибка сжатия! " & Date & " " & Time
Close #1
MsgBox Err.Description
' В случае ошибки, не связанной с подключением пользователей к базе,
' на экране монитора вас будет ждать сообщение с ее описанием
   Err.Clear
End Sub
```

Вообще говоря, такую программу можно написать и прямо в MS Access. Но опыт показал, что вспомогательный файл *.mdb, в котором будет находиться

программа, может быть поврежден в результате многократных запусков, при этом вы не сразу заметите проблему. Для его восстановления потребуется еще одна процедура, запускаемая из отдельного файла базы данных или вручную из приложения MS Access. Созданный в Visual Basic exe-файл не подвержен повреждениям от многократных запусков.

Настроив планировщик заданий на регулярный запуск этой программы, вы забудете о ее работе, поскольку ваша база данных никогда не потребует сжатия вручную из-за появления сбоев в ее работе. Аналогичный подход следует применять и к обслуживанию других программ, систем и сервисов, работающих в сети. Чем больше процедур вы сможете автоматизировать, тем меньше состояние сети будет зависеть от забывчивости или занятости другими проблемами администратора и его помощников.

При наличии подключения к Интернету (и даже без такого подключения) одним из самых востребованных сервисов в сети является электронная почта. Наличие электронной почты служит не только средством общения пользователей между собой и через Интернет, но и инструментом доставки администратору сообщений о состоянии сети и идущих в ней процессов.

Электронная почта в сети

До появления операционной системы Windows Server 2003 организация полноценного почтового сервиса была возможна с помощью программ других разработчиков. Теперь настройка почтового сервера в сети не требует поиска специальной программы — почтового сервера.

Почтовые сообщения, как и само подключение к Интернету, ставит безопасность информации в сети под угрозу, если не предусмотреть определенные меры и средства защиты от возможных проблем. Одна из мер, которую следует принять при организации почты и подключения к Интернету, это размещение таких сервисов на отдельном сервере. В нашем случае это вспомогательный сервер Windows Server 2003.

Компьютер, работающий под Windows Server 2003, который мы применим для организации почтового сервера — дополнительный сервер, который входит в домен, но не является дополнительным контроллером домена. На этой машине могут быть созданы локальные учетные записи пользователей.

Почтовая служба Windows Server 2003 содержит SMTP- и POP3-серверы, а также Web-интерфейс для управления POP3-сервером. Все операции по установке сервисов необходимо выполнять под учетной записью администратора компьютера. SMTP-сервер (Simple Mail Transfer Protocol, простой почтовый протокол передачи данных) входит в состав служб Интернета (IIS), а POP3-

сервер (Post Office Protocol v.3, почтовый протокол Интернета) — в состав сервера приложений для Windows Server 2003. Рассмотрим уже настроенную почтовую службу с необходимыми комментариями.

Примечание

Следует заметить, что ошибки, допущенные при настройке почтовых сервисов, иногда трудно исправить, изменяя те или иные параметры. Лучше всего при возникновении необъяснимых проблем в процессе настройки удалить службы, а затем установить их снова. В дальнейшем, когда почтовый сервис заработает нормально, изменение рабочих параметров службы проблем не вызовет.

Мастер настройки сервера

Как обычно, в серверных системах Windows работу лучше начать с запуска мастера настройки сервера (рис. 2.20). Выбрав дополнительную роль — **Почтовый сервер (POP3, SMTP)**, нажимаем **OK** и выполняем указания мастера. Автоматически будут созданы SMTP- и POP3-серверы. Мастер предложит указать метод проверки подлинности и имя домена электронной почты (рис. 2.21).

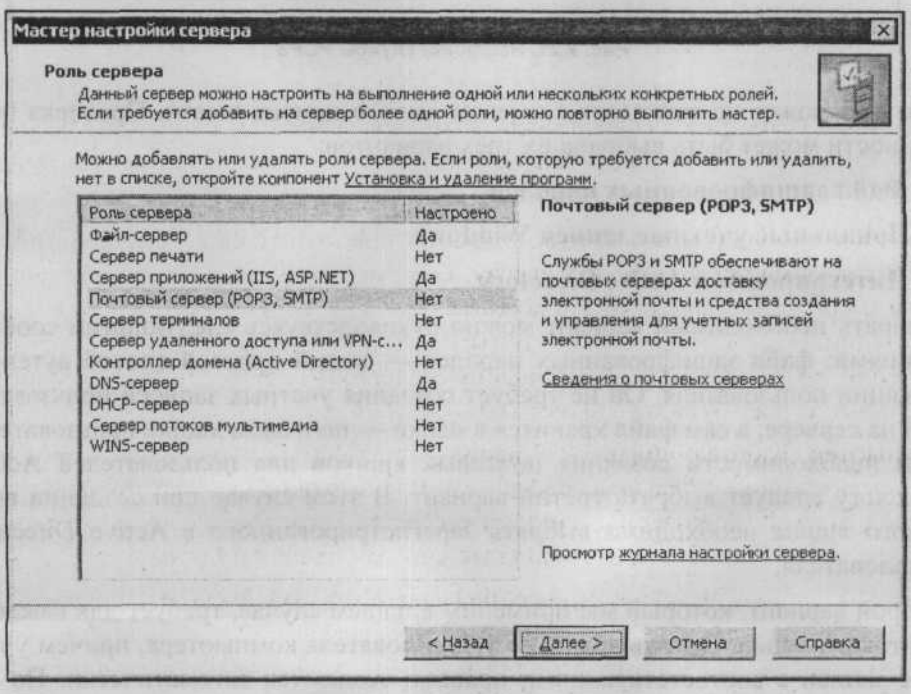

Рис. 2.20. Мастер настройки сервера

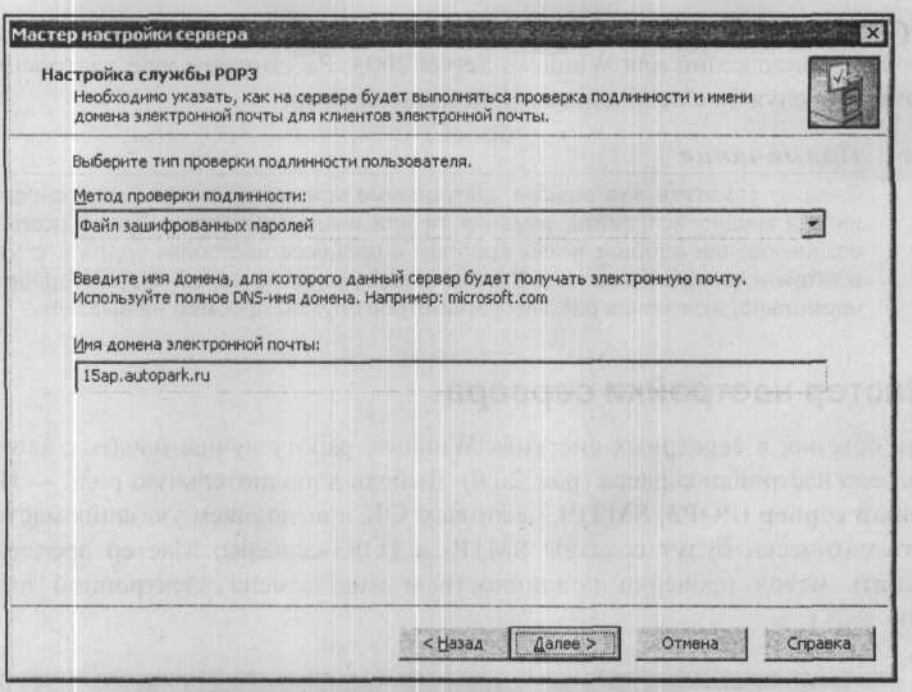

Рис. 2.21. Настройка службы POP3

Это имя может не совпадать с именем вашего домена в сети. Проверка подлинности может быть выбрана их трех вариантов:

- **Файл зашифрованных паролей**.
- **Локальные учетные записи Windows**.
- **Интегрирован в Active Directory**.

Выбрать необходимый вариант можно руководствуясь следующими соображениями: файл зашифрованных паролей — самый простой способ аутентификации пользователя. Он не требует создания учетных записей пользователей на сервере, а сам файл хранится в папке — почтовом ящике пользователя. При необходимости создания почтовых ящиков для пользователей Active Directory следует выбрать третий вариант. В этом случае при создании почтового ящика необходимо выбрать зарегистрированного в Active Directory пользователя.

Второй вариант, который мы применим в нашем случае, требует для каждого почтового ящика создать локального пользователя компьютера, причем учетные записи с соответствующими правами создаются автоматически. По завершении работы мастера можно приступать к созданию почтовых ящиков.

POP3

В средствах администратора появилась возможность управления POP3-сервером (служба POP3). Откройте **Администрирование | Служба POP3** (рис. 2.22).

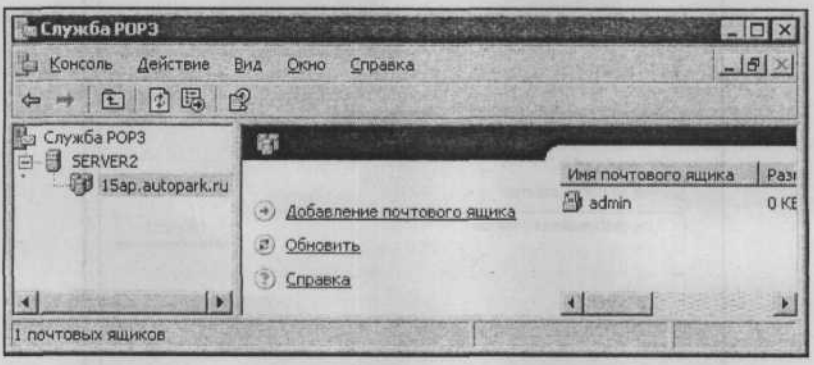

Рис. 2.22. Служба POP3

Если вы решили изменить метод проверки подлинности, то вам придется удалить уже созданный почтовый домен (рис. 2.23).

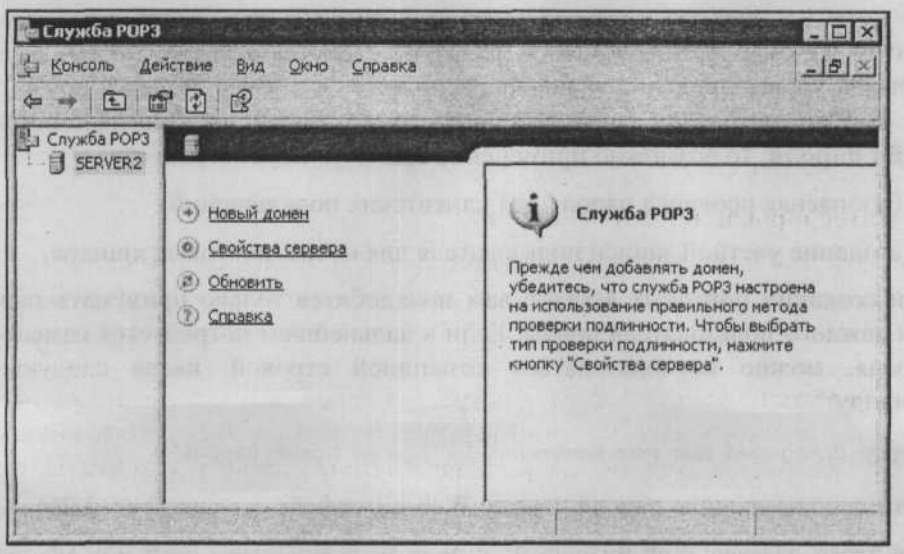

Рис. 2.23. Домен удален, возможно создание нового домена

После этого изменение будет доступно в окне свойств самого POP3-сервера (рис. 2.24).

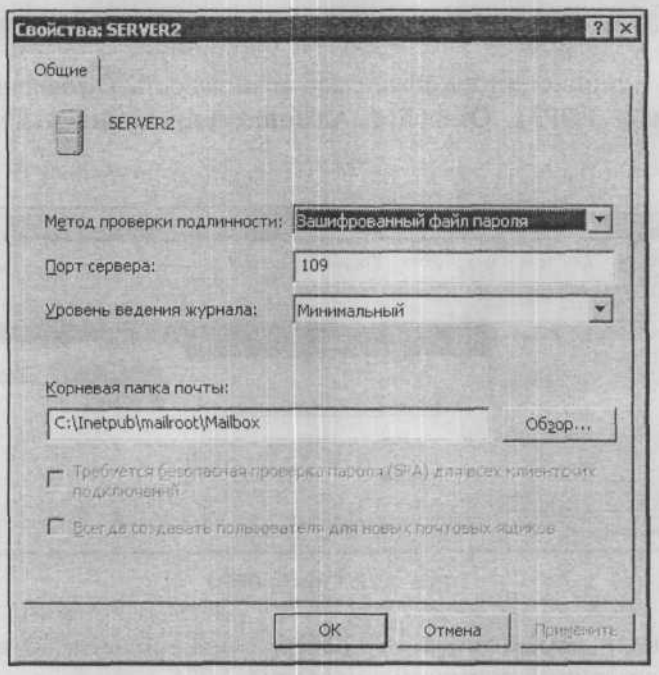

Рис. 2.24. Свойства почтового сервера POP3

В этом же окне можно изменить и другие свойства сервера, такие как порт сервера, уровень ведения журнала, расположение корневой папки почты. Если выбран метод проверки подлинности, отличный от **Зашифрованный файл пароля**, то возможно применение еще двух параметров:

- безопасная проверка пароля для клиентских подключений;
- создание учетной записи пользователя для новых почтовых ящиков.

При создании почтовых ящиков вам понадобится только придумать пароль для каждого пользователя почты. Если в дальнейшем потребуется изменение пароля, можно воспользоваться командной строкой, введя следующую команду:

```
Winpop chengepwd имя_пользователя@имя_домена новый_пароль
```

Возможно изменение пароля и через Web-интерфейс сервера (рис. 2.25).

Для этого, вызвав Web-интерфейс с любого компьютера сети или на самом сервере и перейдя на вкладку **Users**, отметьте нужного пользователя и нажмите кнопку **Set a Password**. На сервере этот интерфейс можно вызвать из меню администратора.

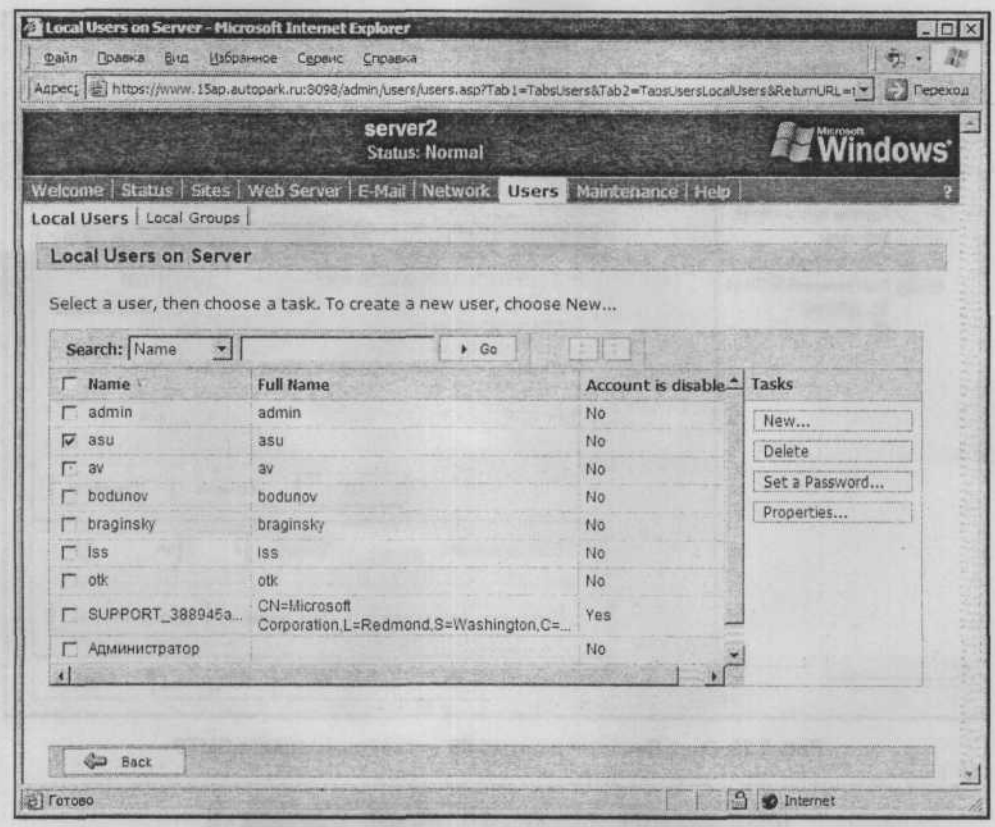

Рис. 2.25. Web-интерфейс для управления пользователями

SMTP

Настроив POP3-сервер, мы получили возможность принимать электронные письма, но для полноценной работы требуется и возможность их отправки. Для этого следует настроить SMTP-сервер (рис. 2.26).

Доступ к настройкам этого сервера можно получить через Диспетчер служб IIS. После установки почтовых служб в окне диспетчера появится объект — **Виртуальный SMTP-сервер**. По умолчанию домену будет дано имя компьютера (интернет-сервера). Вы можете создать любое число доменов с именами, которые зарегистрированы в DNS глобальной сети или в вашей сети. В свойствах сервера можно указать параметры, назначение которых понятно из их названий, но обычно можно применить все значения по умолчанию. Обязательно требуются настройки параметров доступа к серверу и дополнительная настройка доставки (рис. 2.27).

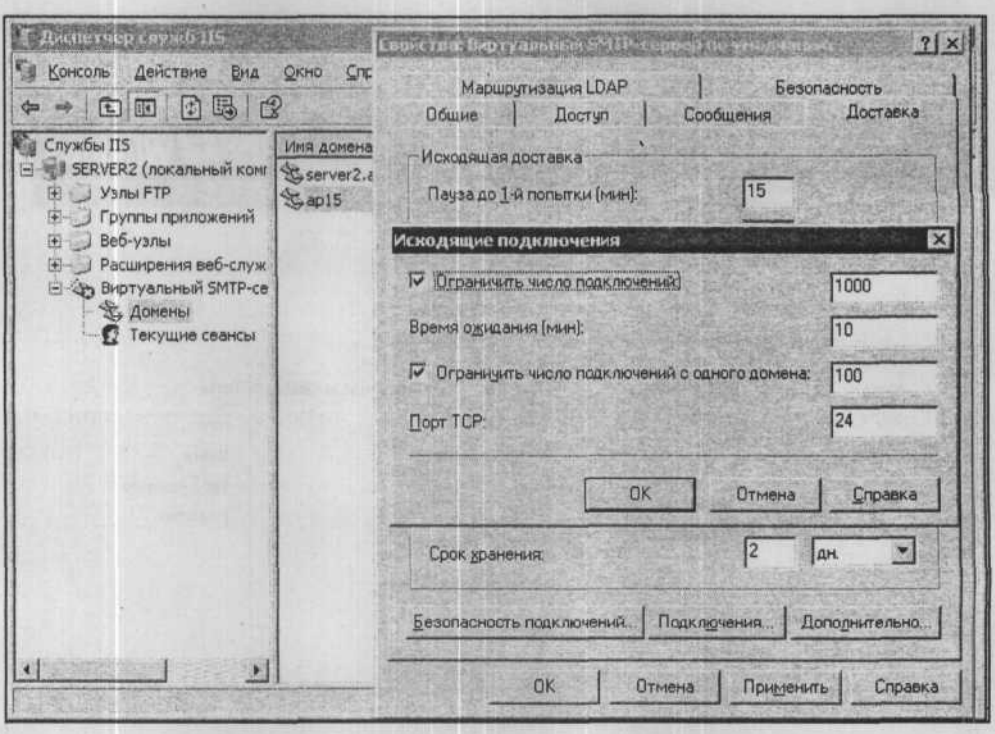

Рис. 2.26. Окно **Диспетчер служб IIS** — свойства сервера SMTP

Рис. 2.27. Дополнительная настройка доставки

Если имя вашего интернет-сервера не зарегистрировано в глобальной сети Интернет, а для почтового сервера используется иное имя, то необходимо указать это имя в поле **Имя подменяющего домена**. Это имя будет использовано почтовым сервером для сообщения своего имени другим серверам Интернета. Направляющий узел — это имя сервера, на который могут отправляться DNS-запросы, когда ваш сервер не сможет их разрешить самостоятельно.

Примечание

Если в поле **Направляющий узел** включить имя вашего сервера, то отправка писем может быть нарушена. Лучше оставить поле пустым.

Более тонкие настройки вы сможете осуществить позднее. После завершения большого числа настроек, а особенно после удаления и добавления новых доменов, следует остановить службу IIS Admin и запустить ее заново. Иногда это не удается, тогда следует перезагрузить компьютер. После этого переходите к настройке почтовых клиентов.

О пользователях

Если почтовый сервер настроен, то основная задача администратора заключается в поддержании его в работоспособном состоянии и управление учетными записями пользователей почтового сервиса. Мы выбрали вариант настройки сервера, когда каждому его пользователю ставится в соответствие локальная учетная запись. Это позволяет при авторизации на почтовом сервере вводить иные данные, чем при входе в сеть, что дополнительно защищает эти данные от попыток их перехвата. Отправка почты также требует авторизации, что не позволит использовать SMTP-сервер посторонним (в том числе распространителям спама), если сервер всегда подключен к Интернету.

Все пользователи, учетные записи которых сформированы во время создания почтового ящика, входят в особую группу POP3Users, члены которой не имеют возможности войти в систему ни локально, ни через сеть. При необходимости, вы можете пользователя почты включить в другие группы на сервере и дать ему другие права.

Примечание

После автоматического создания учетной записи, соответствующей почтовому ящику, необходимо открыть свойства учетной записи и установить флажок **Срок действия пароля не ограничен**, если это необходимо. По умолчанию политика паролей настроена таким образом, что без этой операции пароль станет недействительным через 14 дней. Можно изменить эту политику и срок действия пароля по умолчанию вплоть до неограниченного.

Администрирование сети и почтовый сервис

Наличие почтового сервиса в сети позволяет использовать его для отправки служебных сообщений администратору в автоматическом режиме. О чем вы хотите получать сообщения — это дело вкуса и воображения. Трудно оперативно просмотреть слишком большое количество информации по электронной почте и принять соответствующее ситуации решение. Тем не менее данные об аварийном состоянии системы или сообщения, помогающие отладить процедуры в сети, а также сведения о наиболее важных событиях в сети могут быть полезны. Кроме получения информации о состоянии сети, средства электронной почты позволяют активно взаимодействовать с сетью, находясь на значительном удалении. Такой вариант взаимодействия иногда может быть рискованным, но очень полезным. Важно только заранее определить круг задач, которые вы планируете решить таким путем.

"Лень — двигатель прогресса"

Десятки раз я убеждался в верности этой поговорки. Меня неоднократно вызывали на работу поздно вечером и в выходные дни. Некоторые процессы, зависящие от качества связи с удаленной сетью по выделенной линии, время от времени прерывались. Приходилось искать причины возникшей проблемы, и часто это затягивалось надолго. Обнаружить причины удавалось не всегда (вернее, они заключались во временном ухудшении качества связи), связь восстанавливалась самостоятельно, а потерянного времени было жалко. Очень хотелось получить возможность удаленно контролировать параметры подключений, вводить и выполнить на сервере ту или иную команду. Существуют различные средства удаленного администрирования, о некоторых мы уже говорили. Но для работы с этими средствами требуется более или менее приличная связь с сервером. Если при подключении к удаленному серверу через Terminal Service произойдет обрыв связи, то сеанс останется запущенным на сервере; можно использовать еще один, но в конце концов количество сеансов, допустимое лицензионной политикой, будет исчерпано. Потребуется присутствие оператора у консоли сервера для отключения лишних сеансов. Медлительность других средств удаленного управления и администрирования при плохой связи создает риск подачи ложной команды. Как выяснилось, не только у меня возникали такие проблемы. В ряде случаев, особенно в отдаленных от крупных городов населенных пунктах, администратору приходится обслуживать две или более сетей, находящихся на значительном удалении друг от друга. При этом узнать о состоянии сервера или выполнить какие-либо операции по обслуживанию сети можно, только преодолев значительное расстояние.

Тем не менее есть способ, позволяющий администратору выполнять некоторые процедуры, находясь вне своей сети, но имея доступ к электронной почте. Для реализации этого способа необходимо обеспечить возможность автоматического приема и отправки почты со стороны удаленной сети. Кроме почтового сервера, нам потребуется консольный почтовый клиент. На сайте **http://ironfist.at.tut.by/** предложен очень компактный (менее 50 Кбайт) и, как показала практика, надежный консольный почтовый клиент ZeRAT. Применять его для работы с обычной электронной почтой при установленной на вашем компьютере ОС Windows большого смысла нет (если только вы не почитатель командной строки), поскольку существующие распространенные почтовые клиенты вполне удовлетворяют запросам пользователей. Но это — консольный почтовый клиент, интерфейс для работы с ним — командная строка.

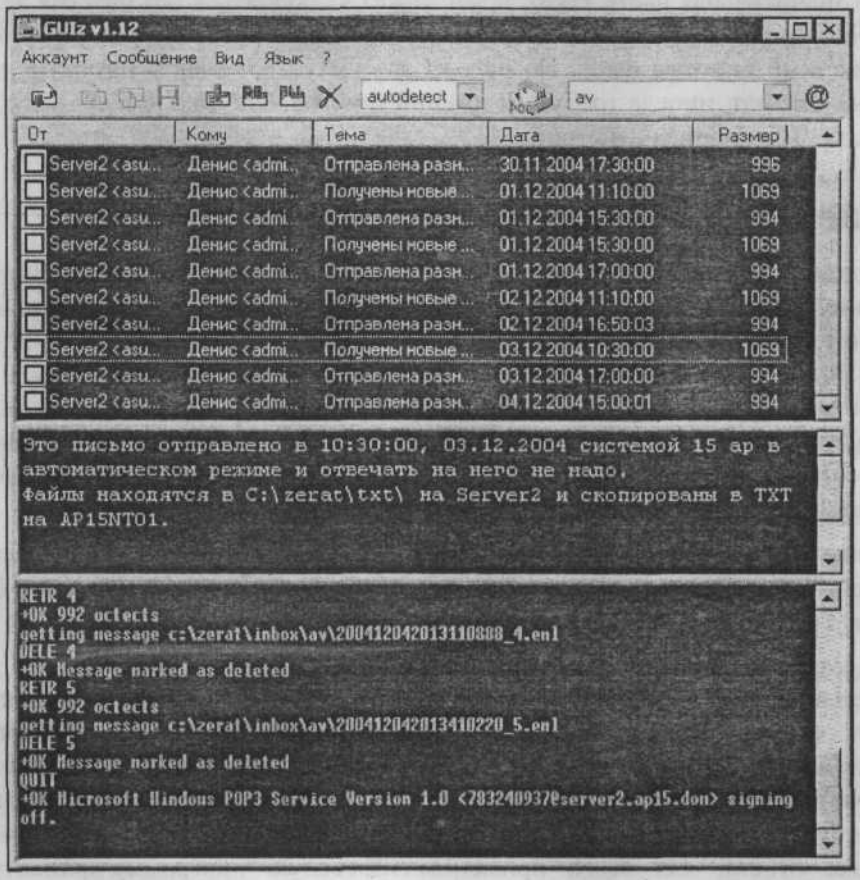

Рис. 2.28. Графическая оболочка GUIz для почтового клиента ZeRAT

Для тех, кому требуется графическая оболочка (рис. 2.28), смогут ее найти на том же сайте. Ее применение даст возможность оперативно просматривать тексты сообщений, полученных с сервера.

С распространением Windows роль командной строки для обычных пользователей ПК постепенно отодвигается на второй план. Тем не менее новые операционные системы позволяют выполнять множество операций, в том числе и связанных с администрированием сети и сервера, из командной строки. Для сохранения заготовок команд можно применить обычные командные (пакетные) файлы с расширением bat или cmd.

В чем состоят наиболее распространенные задачи администрирования сети и сервера? Необходимо в определенный момент времени (или при наступлении определенных условий) получить информацию о состоянии сервера, сети или какой-либо программы и, приняв решение, выполнить ту или иную операцию. Значительная часть таких задач может выполняться без участия человека. Например, антивирусный монитор способен обнаружить и уничтожить зараженный вирусом файл. Но не всегда удается возложить принятие решения на автомат, иногда требуется именно участие человека или его уведомление о произведенном действии.

Решение задач администрирования по E-mail

Для демонстрации работы программы ZeRAT и возможностей администрирования по E-mail решим простую задачу: вы находитесь вне администрируемой сети, необходимо проверить связь сервера с одной из рабочих станций, IP-адрес которой вам известен. Для контроля наличия такой связи применяется обычная команда ping, но ее применение возможно, когда есть доступ непосредственно к серверу. Нам требуется послать на сервер сообщение, содержащее необходимую команду. Сервер, выполнив команду, должен отправить на адрес администратора результат выполнения команды.

Прежде всего, необходимо на почтовом сервере ввести служебную учетную запись, куда будут приходить сообщения с командами; пусть это будет admin@popdomayn.

Следует учесть, что от спама не застрахован ни один почтовый адрес. Ваш сервер не исключение, поэтому необходимо обеспечить обработку только тех писем, которые пришли от вас. Как вариант, можно применить для пересылки вложений ZIP-файл с определенным именем, например, admins.zip. Все другие вложения будут извлекаться, но никаких действий с ними выполняться не будет. Серверу придется создавать этот файл самостоятельно при подготовке ответа, для этого применим известную программу-архиватор — pkzip.exe. Если вы используете другой архиватор для работы в командной

строке, то потребуется скорректировать команды, которые приведены в данном описании.

Для настройки ZeRAT требуются несколько конфигурационных файлов. Рассмотрим настройки применительно к нашему случаю. Будем считать, что вы установили ZeRAT в каталоге C:\zerat\. В листинге 2.3 приведено содержание файла Zerat.ini.

Листинг 2.3. Файл Zerat.ini

```
;SMTP parameters
HELO:smtpdomayn          ; почтовый домен
SMTPHOST: smtpdomayn     ; почтовый домен [:25]
SMTPAuth:login           ; Указание на необходимость аутентификации
SMTPUSER:admins          ; Имя учетной записи почты
SMTPPASS:password        ; пароль доступа
ATTACHEN:BASE64          ; метод кодирования вложений
CHARSET:Windows-1251     ; кодировка текста
```

В листинге 2.4 приведено содержание файла admins.txt, в котором имеются все сведения, необходимые для создания и отправки автоматического сообщения.

Примечание

Программа ZeRAT имеет возможность прямой отправки сообщений без применения SMTP-сервера. Для этого в файле Zerat.ini следует все параметры, начинающиеся с SMTP, оставить без значений, но добавить строку, содержащую адрес доступного DNS-сервера — `DNS:<IP-адрес dns-сервера>`. Тем не менее для приема почтовых отправлений, содержащих команды управления, необходим локальный POP3-сервер.

Листинг 2.4. Файл admins.txt

```
Host: smtpdomayn
From:Сервер admins@popdomayn ; адрес отправителя (сервера)
To:Ваше имя <ваш почтовый адрес>
Type:multipart/mixed
Subject: Сообщение сервера    ;тема сообщения
charset:Windows-1251
$boun                         ;начало текста письма
Content-type: text/plain; charset=Windows-1251
Это письмо отправлено в %Time, %Date в автоматическом режиме и отвечать
на него не надо.
$incl admins.zip              ; Указание на прикрепляемый файл
```

Для того чтобы сервер мог обработать ваше сообщение, к нему потребуется описание его действий в bat-файле. Листинг 2.5 представляет файл IN.bat, который должен запускаться планировщиком Windows через определенные вами интервалы. Сервер проверит наличие сообщения в почтовом ящике и даст команду на прием почты программой ZeRAT.

Листинг 2.5. Файл IN.bat

```
if not exist C:\<путь к почтовому ящику admins>\*.eml    goto d
zerat.exe pop.ini
unzip.bat
:d
```

Для того чтобы сервер знал, откуда принять почту, создадим файл pop.ini (листинг 2.6).

Листинг 2.6. Файл pop.ini

```
EXTRACT:YES   ;Указание на необходимость извлечь вложение
POP3HOST: pop3_server_name:NNNNN       ; имя почтового pop-сервера[:port]
POP3USER:admins@popdomayn          ;учетная запись pop3-сервера
POP3PASS:password          ; pop3-пароль
LOCALDIR:C:\zerat\inbox    ; путь к входящим сообщениям
MESSAGES:delete            ; удалить сообщение с сервера
POP3Auth:regular           ; обычный метод аутентификации
```

В файле in.bat содержится ссылка на файл unzip.bat (листинг 2.7). Этот файл необходим для распаковки вложения и выполнения дополнительных команд.

Листинг 2.7. Файл unzip.bat

```
if not exist C:\zerat\inbox\admins.zip goto d
pkzip -extr=up c:\zerat\inbox\admins.zip
copy/y admins.bat C:\zerat\txt\
del c:\zerat\inbox\ admins.zip
admins.bat
```

Приняв и распаковав вложение, удалив файл архива, сервер выполнит файл admins.bat, содержание которого может быть таким, как в листинге 2.8.

Листинг 2.8. Файл admins.bat

```
Ping <IP-адрес> > mess.txt
Out.bat
```

Результат выполнения команды будет записан в файл mess.txt, который сервер отправит вам. Команды для отправки сообщения должны быть записаны в файле out.bat, содержание которого приведено в листинге 2.9.

Листинг 2.9. Файл out.bat

```
if not exist mess.txt goto d ;если нет mess.txt, прекращаем выполнение
pkzip -add c:\zerat\admins.zip mess.txt;Архивируем файл
zerat.exe admins.txt ; отправляем архив на ваш адрес
del c:\zerat\mess.txt ; удаляем более не нужные файлы
del c:\zerat\admins.zip
:d
```

Получив сообщение и прочитав результат выполненной команды, вы можете написать новый bat-файл с другими командами и отправить его серверу. Все сообщения, полученные сервером, будут храниться в каталоге C:\zerat\inbox\.

Несколько модифицируя описанные файлы и добавляя новые, можно заставить сервер посылать подтверждения о приеме ваших команд или промежуточные сообщения в процессе выполнения предписанных операций.

Среди команд командной строки в новых операционных системах, начиная с Windows XP, появилось много новых. Возможности некоторых из них сравнимы с возможностями отдельных программ. Например, появился целый комплекс команд Netsh (diag). Эти команды подробно описаны в справочной системе, а здесь рассмотрим одну, позволяющую протестировать доступность какого-либо компьютера.

В командной строке можно написать следующее:

```
netsh diag connect iphost mail.company.com 25
```

Это значит, что мы подключаемся к узлу mail.company.com по порту 25 для проверки связи. Если перенаправить результат выполнения команды в файл, то его содержание будет следующим:

```
IPHost (mail.company.com)
 IPHost = mail.company.com
 Port = 25
 Сервер запущен с порта [25]
```

Получив такой текст по электронной почте, вы будете уверены, что ваш сервер имеет возможность подключения к SMTP-серверу mail.company.com.

Если заранее подготовить несколько вспомогательных bat-файлов, можно упростить написание команд для сервера. Допустим, вам часто требуется проверять связь сервера с какими-либо компьютерами в сети или с другими

серверами. Вы можете в качестве заготовки для команд написать следующий файл ipscan.bat, представленный в листинге 2.10, и отправить его на сервер (процедуру отправки опишем позднее).

Листинг 2.10. Файл ipscan.bat

```
netsh diag connect iphost %1% 25
netsh diag connect iphost %1% 110
netsh diag connect iphost %1% 53
netsh diag connect iphost %2% 25
netsh diag connect iphost %2% 110
netsh diag connect iphost %2% 53
netsh diag connect iphost %3% 25
netsh diag connect iphost %3% 110
netsh diag connect iphost %3% 53
netsh diag connect iphost %4% 25
netsh diag connect iphost %4% 110
netsh diag connect iphost %4% 53
```

В этом файле несколько раз перечислена одна и та же команда, но с различными параметрами. Если вы поместите этот файл в каталог C:\zerat\, то для выполнения сканирования по нескольким адресам вам понадобится файл admins.bat, показанный в листинге 2.11.

Листинг 2.11. Файл admins.bat с перечнем из четырех адресов

```
ipscan 195.34.32.10 212.188.4.10 194.67.18.127 212.48.140.154 >mess.txt
out.bat
```

Как видно, написание командного файла существенно упростилось. В ответ на свое послание вы получите файл mess.txt с результатом работы вашей команды (листинг 2.12).

Листинг 2.12. Файл mess.txt с результатом выполнения команды

```
C:\zerat>netsh diag connect iphost 195.34.32.10 25
IPHost (195.34.32.10)
    IPHost = 195.34.32.10
    Port = 25
    Сервер запущен с порта [Отсутствует]
C:\zerat>netsh diag connect iphost 195.34.32.10 110
IPHost (195.34.32.10)
    IPHost = 195.34.32.10
```

```
    Port = 110
    Сервер запущен с порта [110]
C:\zerat>netsh diag connect iphost 195.34.32.10 53
IPHost (195.34.32.10)
    IPHost = 195.34.32.10
    Port = 53
    Сервер запущен с порта [53]
C:\zerat>netsh diag connect iphost 212.188.4.10 25
IPHost (212.188.4.10)
    IPHost = 212.188.4.10
    Port = 25
    Сервер запущен с порта [Отсутствует]
C:\zerat>netsh diag connect iphost 212.188.4.10 110
IPHost (212.188.4.10)
    IPHost = 212.188.4.10
    Port = 110
    Сервер запущен с порта [110]
C:\zerat>netsh diag connect iphost 212.188.4.10 53
IPHost (212.188.4.10)
    IPHost = 212.188.4.10
    Port = 53
    Сервер запущен с порта [Отсутствует]
C:\zerat>netsh diag connect iphost 194.67.18.127 25
IPHost (194.67.18.127)
    IPHost = 194.67.18.127
    Port = 25
    Сервер запущен с порта [25]
C:\zerat>netsh diag connect iphost 194.67.18.127 110
IPHost (194.67.18.127)
    IPHost = 194.67.18.127
    Port = 110
    Сервер запущен с порта [110]
C:\zerat>netsh diag connect iphost 194.67.18.127 53
IPHost (194.67.18.127)
    IPHost = 194.67.18.127
    Port = 53
    Сервер запущен с порта [Отсутствует]
C:\zerat>netsh diag connect iphost 212.48.140.154 25
IPHost (212.48.140.154)
    IPHost = 212.48.140.154
    Port = 25
    Сервер запущен с порта [25]
```

```
C:\zerat>netsh diag connect iphost 212.48.140.154 110
IPHost (212.48.140.154)
    IPHost = 212.48.140.154
    Port = 110
    Сервер запущен с порта [110]
C:\zerat>netsh diag connect iphost 212.48.140.154 53
IPHost (212.48.140.154)
    IPHost = 212.48.140.154
    Port = 53
    Сервер запущен с порта [Отсутствует]
```

Просмотрев внимательно содержание файла, можно сделать выводы о работе просканированных узлов, представленные в табл. 2.1.

Таблица 2.1. *Обработанный ответ сервера*

IP \ сервис	POP3 (110)	SMTP	DNS
195.34.32.10	Да	Нет	Да
212.188.4.10	Да	Нет	Нет
194.67.18.127	Да	Да	Нет
212.48.140.154	Да	Да	Нет

Среди команд, которые может выполнить сервер, допустима и такая:

```
shutdown -r -f -m \\MyServer -t 60 -d up:125:1
```

Эта команда позволяет закрыть все работающие программы и через 60 с перезагрузить сервер. Применяя эту команду, следует быть уверенным, что перезагрузка в данный момент допустима. Учитывая, что почтовый адрес для управления сервером может стать известным, не используйте приведенные имена файлов admins.zip и admins.bat. Придумайте имена, которые невозможно повторить случайно или подобрать. Проверяйте содержимое папки inbox на наличие в ней чужих сообщений. При удаленном управлении неплохо заставить сервер посылать подтверждения о получении сообщений. Если вы получите подтверждение, но сами не посылали сообщений, следует внимательно просмотреть чужие послания, определив их источник. Запретите доступ к папке C:\zerat обычным пользователям.

Теперь рассмотрим процедуру отправки заготовленных для выполнения команд. Для пересылки дополнительного файла его следует упаковать вместе с admins.bat в admins.zip. После получения этой посылки сервер распакует все файлы в C:\zerat\. Если вам необходимо сразу выполнить подготовленные команды, то содержание admins.bat подобно приведенному в листинге 2.11.

Если требуется только переслать файлы и получить об этом уведомление, то файл admins.bat может быть таким, как показано в листинге 2.13.

Листинг 2.13. Файл admins.bat с добавлением заготовленных команд

```
dir c:\zerat\txt /on c:\zerat\*.bat >mess.txt
out.bat
```

Получив ответ (листинг 2.14), вы сможете убедиться, что все файлы лежат на своих местах.

Листинг 2.14. Файл mess.txt с перечнем bat-файлов

```
Том в устройстве C не имеет метки.
 Серийный номер тома: 0936-D08A

 Содержимое папки c:\zerat\txt

09.06.2004  21:58    <DIR>          ..
09.06.2004  21:58    <DIR>          .
09.06.2004  22:06                60 admins.bat
               1 файлов             60 байт

 Содержимое папки c:\zerat

09.06.2004  22:06                60 admins.bat
01.06.2004  09:33                32 IN.bat
09.06.2004  20:18               410 ipscan.bat
01.06.2004  09:05                64 OUT.bat
               4 файлов            566 байт
               0 папок  21 226 254 336 байт свободно
```

Вариант применения команды `dir` в данном случае позволяет вывести только имена командных файлов, находящихся в каталогах C:\zerat\txt\ и C:\zerat\. Надеюсь, что приведенных примеров достаточно, чтобы представить себе возможности администрирования сети по электронной почте, но еще на одну такую возможность следует указать. Почтовые сообщения от сервера могут быть достаточно краткими, чтобы использовать для чтения... сотовый телефон! Теперь, настроив свой мобильный телефон на прием электронной почты, вы сможете всегда получать сведения о состоянии сервера, независимо от своего места нахождения.

Раз уж нам удалось заставить сервер отвечать на наши письма, то, скорее всего, вы без труда напишете несколько строк в bat-файле для отправки вам сообщения по команде планировщика задач, что позволит вам быть в курсе со-

бытий, происходящих на сервере. На рис. 2.27 именно это и показано. Сервер отправил сообщение о выполнении операции с файлами. То, о чем я мечтал, когда меня вызывали по выходным, теперь работает. Сервер сообщает мне и моему помощнику о работе важного процесса в сети. Если в один из дней не окажется таких сообщений до определенного часа, — это повод для выяснения ситуации сначала по телефону, а затем средствами удаленного администрирования. Во всяком случае, теперь нет необходимости, на ночь глядя, срочно выезжать по вызову к серверу.

SMS-сообщения из сети

В Интернете можно найти много программных средств, предназначенных для отправки sms-сообщений с компьютера. Некоторые из них используют не стандартизованные свойства программ операторов связи. Поэтому никто не может гарантировать, что завтра не произойдут изменения, которые не позволят вашей программе работать правильно. Другие программы ориентируются на специально созданные шлюзы в Интернете, и их поддержка требует средств, которые платят пользователи, приобретая программу. Единственным надежным и независимым от свойств шлюзов в Интернете средством для отправки sms-сообщений с применением компьютера в настоящее время можно считать сам мобильный телефон.

Microsoft бесплатно предлагает программу SMS Sender (рис. 2.29), которая позволяет готовить сообщение на компьютере, а затем через интерфейсный кабель RS-232 передавать его на мобильный телефон для отправки.

Программа SMS Sender может быть использована в режиме командной строки. Для этого необходимо запустить файл smssender.exe с указанием требуемых параметров. Программа применяет устройство, которое было использовано при предыдущем запуске. Данная возможность позволяет автоматизировать отправку сообщений.

Использование:

```
smssender.exe [[/i] /p:<телефон> /m:"<сообщение>" [/u] [/l]] [/?]
```

где:

`/i` — номер телефона в международном формате;

`/p: <телефон>` — номер телефона (только цифры);

`/m:"<сообщение>"` — текст сообщения в кавычках;

`/u` — кодировка сообщения в UCS-2 (расширенная таблица знаков);

Примечание

По умолчанию используется стандартный алфавит GSM.

`/l` — запись в журнал отправленного сообщения;

`/?` — вывод справки по использованию.

Соответственно, команда

```
smssender /p:8916XXXXXXX /m:"Privet ot servera"
```

позволит вам получить сообщение от сервера, независимо от вашего присутствия около компьютера. Важно лишь, чтобы мобильный телефон был подключен к компьютеру.

Программу можно получить по адресу в Интернете:

http://www.microsoft.com/downloads/details.aspx?FamilyID=06a4f997-7f69-4891-8929-37b9041924a2&displaylang=ru.

Ссылки на нее часто встречаются и на других сайтах, посвященных бесплатным программам.

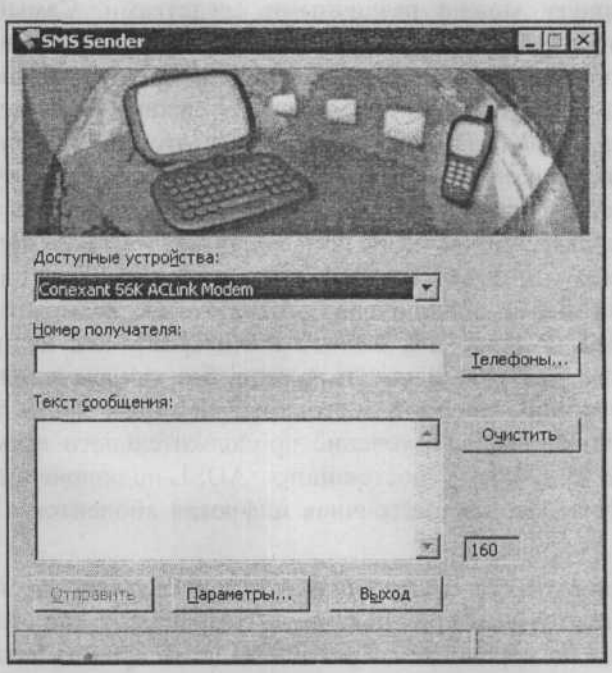

Рис. 2.29. Окно программы SMS Sender

Справедливости ради следует сказать, что не все мобильные аппараты поддерживаются этой программой, да и последовательные порты в последнее время не всегда имеются у компьютеров (или их недостаточно). Если вам не удалось применить мобильный телефон для отправки SMS с сервера, то можно воспользоваться услугой сервиса smsmail.ru. Необходимо зарегистриро-

ваться на сайте **www.smsmail.ru**. После регистрации вы получите возможность бесплатной отправки двух сообщений через электронную почту на адрес <номер мобильного телефона>@smsmail.ru. Сообщения будут приходить на ваш мобильный телефон. Для отправки большего числа сообщений необходимо перечислить на счет, указанный на страницах сайта, оплату в сумме, соответствующей произведению $0,04 * число сообщений.

Как заставить сервер отправлять электронную почту, мы уже рассмотрели ранее.

Интернет для сети

Мы уже рассмотрели применение почтового сервера в сети, а также средства оповещения администратора о событиях в сети. Но эти средства будут не очень полезны, если сеть не имеет выхода в Интернет. Обеспечить подключение к Интернету можно различными средствами. Самый простой вариант — dial-up-подключение через аналоговый модем. Если учесть, что в современных операционных системах есть средства командной строки для запуска процедуры подключения через модем, а также для разрыва установленного подключения, то может применяться этот вид связи с глобальной сетью, хотя довольно ограниченно. К сожалению, низкая пропускная способность такого канала связи и не слишком высокая надежность удержания установленного соединения не позволяют использовать такое подключение для обеспечения работы почтового и Web-сервисов в сети. Еще один существенный недостаток dial-up-подключения — отсутствие возможности использовать постоянный IP-адрес для выхода в Интернет, что не позволяет применять сервисы, доступные из Интернета без привлечения специальных средств, позволяющих получить постоянный IP-адрес. Кроме того, оплата за непрерывное подключение в течение продолжительного времени окажется намного выше стоимости постоянного ADSL-подключения (Asymmetric Digital Subscriber Line, асимметричная цифровая абонентская линия) за тот же период.

Примем как аксиому, что современная сеть при наличии такой возможности должна иметь постоянное подключение к Интернету, даже если это сеть небольшая. А судя по переписке с читателями, возможность такая есть даже в местах, удаленных от крупных городов на сотни километров. Для кого-то покажется удивительным, но в таежных поселках Сибири функционируют сети с подключением к Интернету через спутник. Оказывается, что дело не в проблемах снабжения или удаленности от цивилизации, а в позиции администраторов этих сетей. В нашей сети применено подключение через ADSL-модем. Настройку такого подключения, обеспечивающую правильную работу сети, мы и рассмотрим.

Организация постоянного подключения к Интернету характеризуется наличием одного или более числа IP-адресов, которые выделены вашей сети для организации шлюза. В большинстве случаев подключение требует наличия лишь одного реального IP-адреса, который будет присвоен сетевому адаптеру, "смотрящему наружу". Кроме собственно адреса, сетевому адаптеру присваивается некая подсеть с маской, отличающейся от других масок во множестве других подсетей. Конкретный адрес сети входит в диапазон адресов, выделяемых провайдером. В пределах этого диапазона адресов создаются подсети, в которые может входить один или больше IP-адресов, которые можно использовать для идентификации компьютера или сервера в Интернете. В рассматриваемом варианте вся подсеть содержит четыре адреса. Первый и последний адреса не могут быть использованы устройствами, аналогично первому и последнему адресам вашей внутренней сети (например, 192.168.115.0 и 192.168.115.255). Для рассматриваемой подсети это могут быть адреса X.X.X.156 и X.X.X.159. Один адрес требуется ADSL-модему, а для использования внешним адаптером сети остается один адрес.

Таблица 2.2. *Внешний адрес вашей сети*

Маска подсети 255.255.255.252 /30 (11111111.11111111.11111111.11111100)	
64 подсети	
Наименьший IP	**Наибольший IP**
x.x.x.0	x.x.x.3
x.x.x.4	x.x.x.7
----------	----------
x.x.x.156	**x.x.x.159**
----------	----------
x.x.x.252	x.x.x.255

В табл. 2.2 показан фрагмент перечня подсетей с маской 255.255.255.252, расширением 30 и с указанием начального и конечного адресов каждой подсети. Расширение 30 показывает число единиц в двоичной записи маски подсети. Только последний октет маски (восемь знакомест в двоичной записи) содержит нули, место которых должны занять цифры из реального адреса. В рассматриваемом примере адреса X.X.X.157 и X.X.X.158 соответствуют в двоичной записи X.X.X.10011101 и X.X.X.10011110. Только два последних знакоместа могут содержать произвольные значения, из которых исключены 00 и 11. Таких произвольных значений остается два. Если по вашему догово-

ру с провайдером вам будет выделено больше адресов, то и маска подсети, и ее расширение будут иными. С полной таблицей подсетей можно ознакомиться в *приложении*. Но в нашем случае внешнему адаптеру может быть присвоен адрес X.X.X.158, а X.X.X.157 назначен ADSL-модему.

Примечание

Распространены и другие варианты подключения компьютеров к Интернету, например, через домовые или городские сети. В этом случае компьютеру, подключенному к этой внешней сети, присваивается один из адресов этой сети. Для подключения локальной сети к Интернету такой вариант не подходит. Вы не сможете зарегистрировать домен второго или третьего уровня, сервером которого будет ваш компьютер.

Итак, мы имеем внешний адрес X.X.X.158, присвоенный внешнему сетевому адаптеру второго сервера, который и будет играть роль шлюза в Интернете для всей сети. Задача — использовать этот адрес для подключения пользователей сети к Интернету. Есть несколько вариантов решения этой задачи, но мы рассмотрим два из них. Первый — подключение с использованием NAT, а второй, как дополнительный, — подключение через прокси-сервер (proxy server).

Подключение к Интернету с применением преобразования сетевых адресов (NAT)

Первый способ подключения наиболее удобен и позволяет, не применяя никакого дополнительного программного обеспечения, предоставить пользователям сети практически все возможности Интернета. Единственное, чего не получат пользователи сети, — это своего IP-адреса при подключении к Интернету. При этом будут недоступны сервисы, для которых необходим персональный IP-адрес. Достаточно упомянуть возможность бесплатной отправки SMS-сообщений со специально созданных для этого Web-страниц. Во многих случаях на них действует ограничение на количество сообщений с одного IP-адреса. Соответственно, такое ограничение будет распространяться на всю сеть. Без специального согласования с вами пользователи не смогут подключаться к своим рабочим компьютерам из дома. Но это ограничение, как только что было сказано, зависит от согласования с вами, и может быть обойдено. Вы можете, настроив соответствующим образом сервер, предоставить такую возможность, если это необходимо. Но самое главное, что такую возможность, которая позволит управлять не только рабочим компьютером, но и серверами сети, вы можете предоставить себе.

Для удобства изложения, вспомогательный сервер с установленной ОС Windows Server 2003, обозначим как интернет-сервер. Отметим, что на интернет-сервере должно быть установлено два сетевых адаптера: один для

подключения к локальной сети, другой — для подключения к ADSL-модему. (В *главе 1* это отмечено на схеме сети.) Говоря о подключении к Интернету, рассмотрим и некоторые вопросы маршрутизации, поскольку высокоскоростное подключение к глобальной сети позволяет использовать ее не только для прогулок по Интернету, но и для доступа к своей собственной сети из Web.

Настроить NAT (Network AddressTranslation, преобразование сетевых адресов) можно с помощью мастера настройки маршрутизации и удаленного доступа. Но никакие мастера не могут обеспечить настройку всех необходимых параметров. Более того, возможно, что на вашем компьютере уже настроена маршрутизация для каких-то целей. Поэтому рассмотрим уже выполненные настройки, отмечая необходимые для доступа в Интернет и для обеспечения доступа извне. Для того чтобы легче ориентироваться в свойствах интерфейсов, следует заранее дать им понятные имена. Это сделать совсем несложно. Войдите в **Панель управления**, откройте **Сетевые подключения** и переименуйте имеющиеся адаптеры, например, как на рис. 2.30.

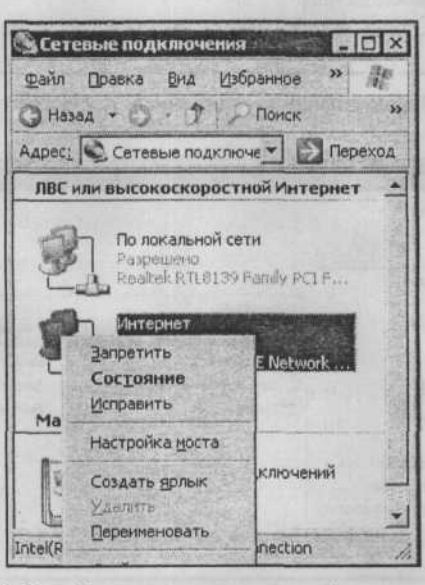

Рис. 2.30. Окно **Сетевые подключения** (переименование)

Один адаптер назовем **Интернет**, а другой — **По локальной сети**. Посмотрите теперь содержимое окна **Маршрутизация и удаленный доступ** (рис. 2.31). Перепутать интерфейсы сети при дальнейших манипуляциях будет невозможно.

Вполне вероятно, что в колонке **Состояние подключения** (четвертая по счету на рисунке) вы увидите иную информацию, если один из интерфейсов

(или оба) не подключены к сети. Это нисколько не помешает довести все настройки до конца, а только потом подключиться к сети. Интерфейсы **Замыкание на себя** и **Внутренний** созданы самим компьютером, и настройка их в нашем случае не требуется. Перейдем по дереву объектов **Маршрутизация и удаленный доступ** к позиции **IP-маршрутизация | Общие** (рис. 2.32).

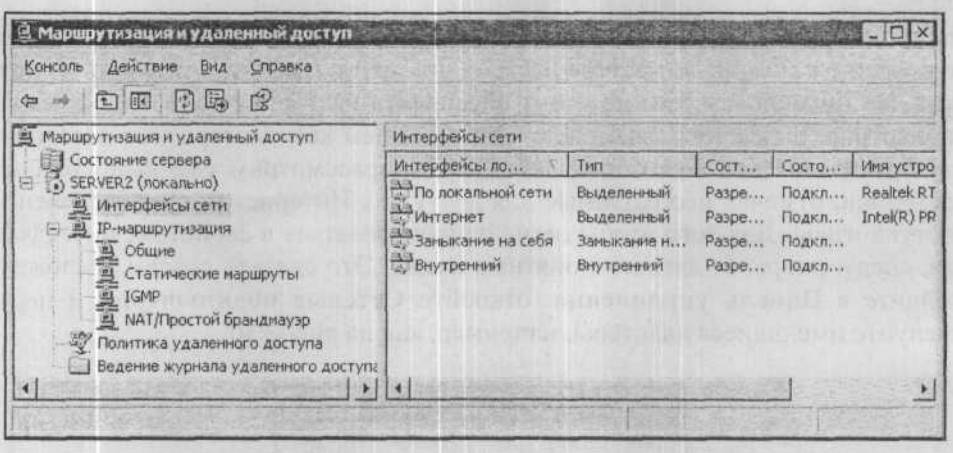

Рис. 2.31. Окно **Маршрутизация и удаленный доступ (Интерфейсы сети)**

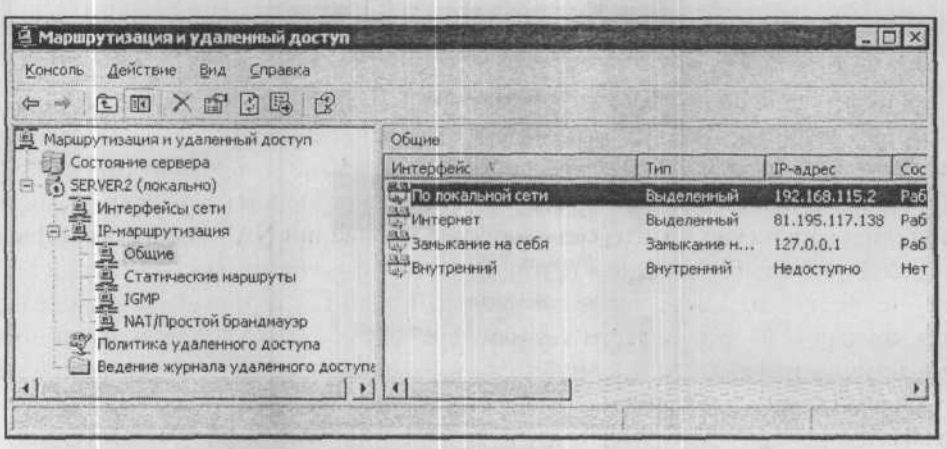

Рис. 2.32. Окно **Маршрутизация и удаленный доступ (IP-маршрутизация | Общие)**

В свойствах интерфейсов, касающихся маршрутизации, видим IP-адреса, которые необходимо присвоить сетевым адаптерам. Рассмотрим свойства интерфейсов. В свойствах интерфейса **По локальной сети** на вкладке **Общие** (рис. 2.33) должен быть выставлен флажок **Включить диспетчер IP-маршрутизации**. Тот же флажок должен быть установлен и в свойствах второго интерфейса.

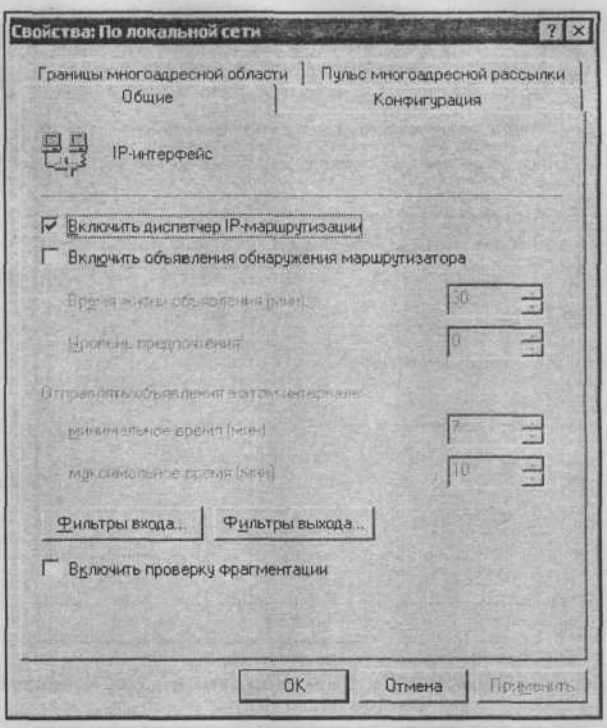

Рис. 2.33. *Окно* **Свойства: По локальной сети**, *вкладка* **Общие**

Перейдем на вкладку **Конфигурация** (рис. 2.34). Именно на этой вкладке можно назначить IP-адрес интерфейсу, если он еще не назначен или назначен иной. Для интерфейса **По локальной сети** должен быть назначен адрес, допустимый в вашей локальной сети. В отличие от простых средств организации общего доступа к Интернету, при использовании NAT мы не ограничены адресом 192.168.0.1 и можем применить любой допустимый в сети адрес. Но лучше, если этот адрес входит в диапазон адресов, который вы определили для серверов. Маска подсети устанавливается соответствующей маске, применяемой в вашей сети. Маршрутизатор (основной шлюз) не указываем, поскольку из сети подключение осуществляется непосредственно к этому интерфейсу.

Для интерфейса **Интернет** необходимо указать IP-адрес, который будет виден из Интернета (рис. 2.35). В данном случае он равен 81.195.117.138, при этом маска подсети — 255.255.255.252. В поле **Маршрутизатор (основной шлюз)** указываем адрес ADSL-модема, поскольку именно через него будет осуществлен выход в Интернет.

Перейдем к следующему объекту дерева в левой части окна **Маршрутизация и удаленный доступ — Статические маршруты** (рис. 2.36).

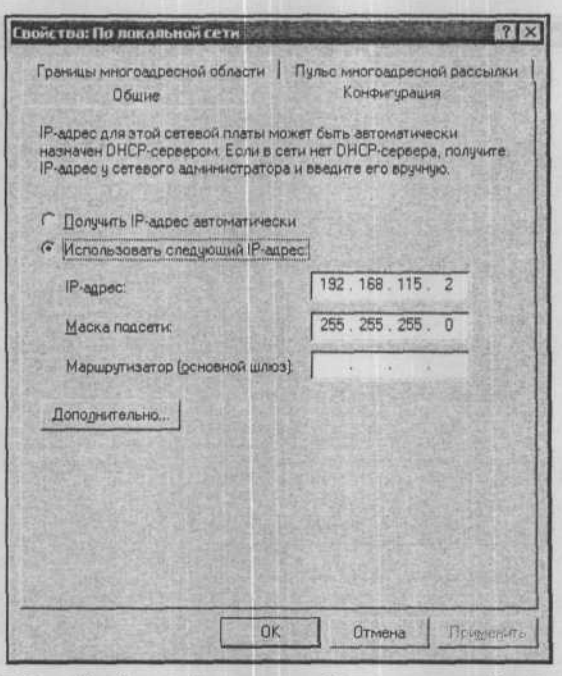

Рис. 2.34. Окно **Свойства: По локальной сети**, вкладка **Конфигурация**

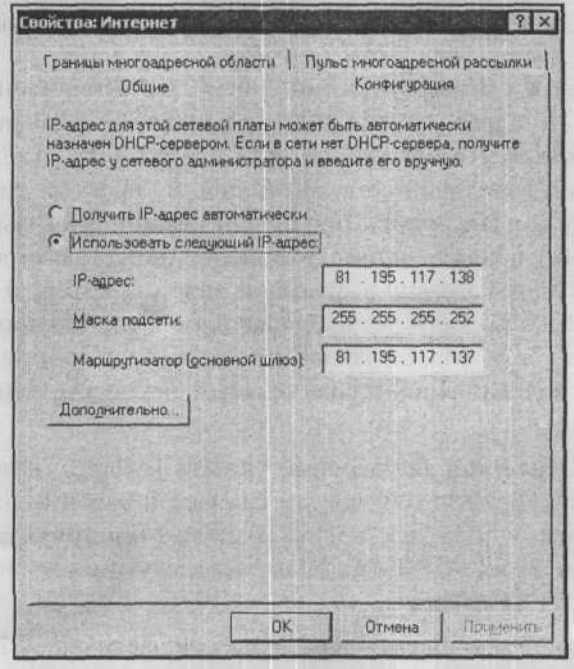

Рис. 2.35. Окно **Свойства: Интернет**, вкладка **Конфигурация**

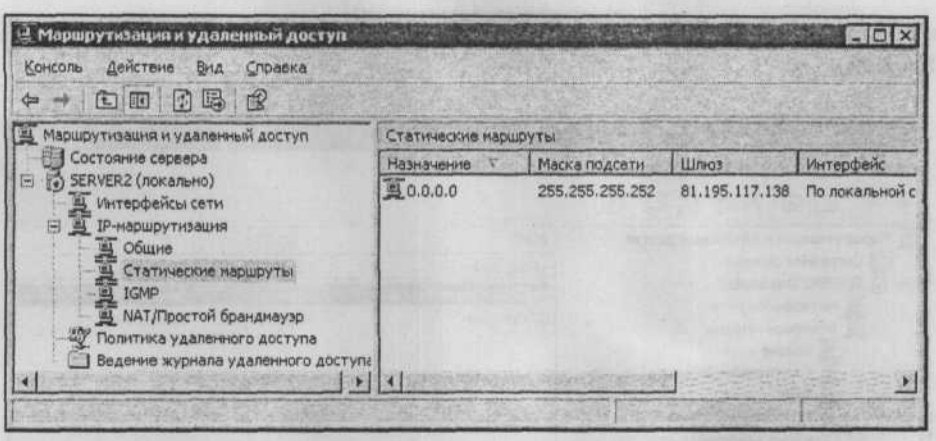

Рис. 2.36. Окно **Маршрутизация и удаленный доступ** (**Статические маршруты**)

Если маршруты не назначены или назначены другие маршруты, вызываем из контекстного меню объекта пункт **Новый статический маршрут**. В появившемся окне (рис. 2.37) выбираем в поле **Интерфейс** опцию **По локальной сети**, в качестве адреса назначения указываем 0.0.0.0, маска подсети 255.255.255.252, а шлюз — адрес интерфейса **Интернет**. Это значит, что все пакеты, полученные из Интернета, будут доступны всем IP-адресам вашей сети, а проходить они должны через интерфейс **Интернет**. **Метрика** уже установлена — "1", и менять это значение нет необходимости.

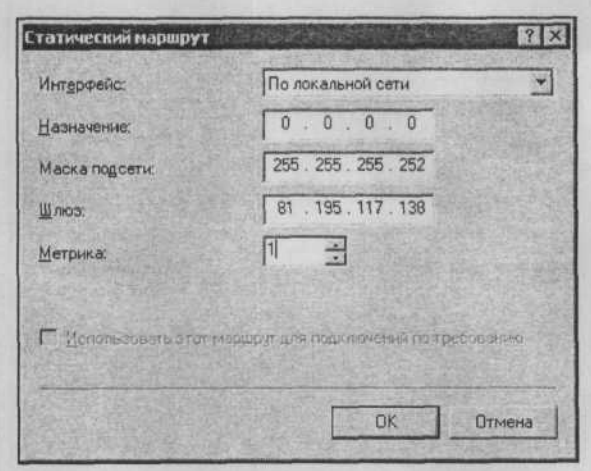

Рис. 2.37. Окно **Статический маршрут**

Следующий объект — **IGMP** (Internet Group Management Protocol, протокол управления группами Интернета). В этом объекте должны быть указаны роли интерфейсов (рис. 2.38). Интерфейс **Интернет** находится в роли маршрутиза-

тора, а интерфейс **По локальной сети** — в роли доверенного интерфейса (**Прокси**).

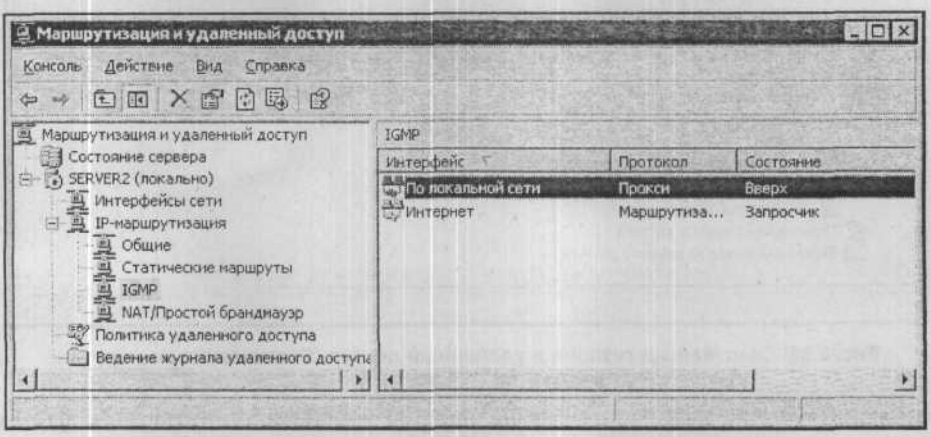

Рис. 2.38. Окно **Маршрутизация и удаленный доступ (IGMP)**

Если это не так, откройте свойства интерфейсов в этом объекте и установите необходимое (рис. 2.39 и 2.40).

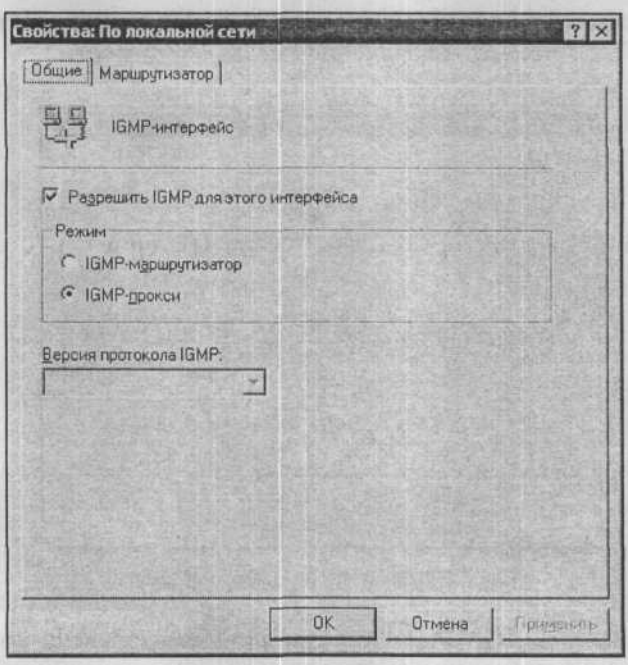

Рис. 2.39. Установка свойств IGMP в окне **Свойства: По локальной сети** на вкладке **Общие**

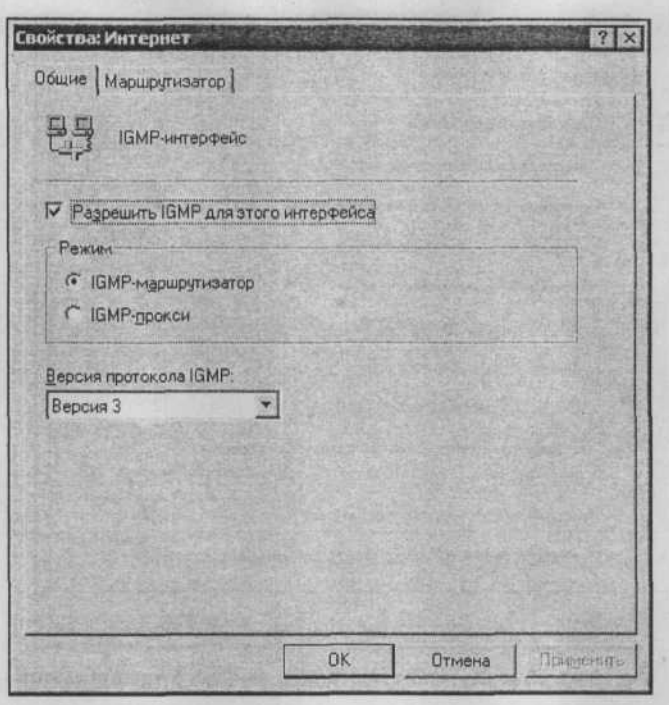

Рис. 2.40. Окно **Свойства: Интернет**, вкладка **Общие**

Для обоих интерфейсов должен быть установлен флажок **Разрешить IGMP для этого интерфейса**, для каждого интерфейса необходимо установить соответствующий режим.

Версию протокола IGMP можно оставить по умолчанию.

На вкладке **Маршрутизатор** для интерфейса **Интернет** (рис. 2.41) по умолчанию устанавливаются еще несколько параметров. Без необходимости их изменять не следует.

И наконец, настроим объект **NAT/Простой брандмауэр** (рис. 2.42). В отличие от Windows 2000 Server, здесь мы можем защитить наше подключение средствами операционной системы.

В свойствах интерфейса **По локальной сети** необходимо указать тип интерфейса — **Частный интерфейс подключен к частной сети** (рис. 2.43).

Для интерфейса **Интернет** (рис. 2.44) должны быть установлены следующие опции:

- **Общий интерфейс подключен к Интернету**
- **Включить NAT на данном интерфейсе**
- **Включить основной брандмауэр для этого интерфейса**

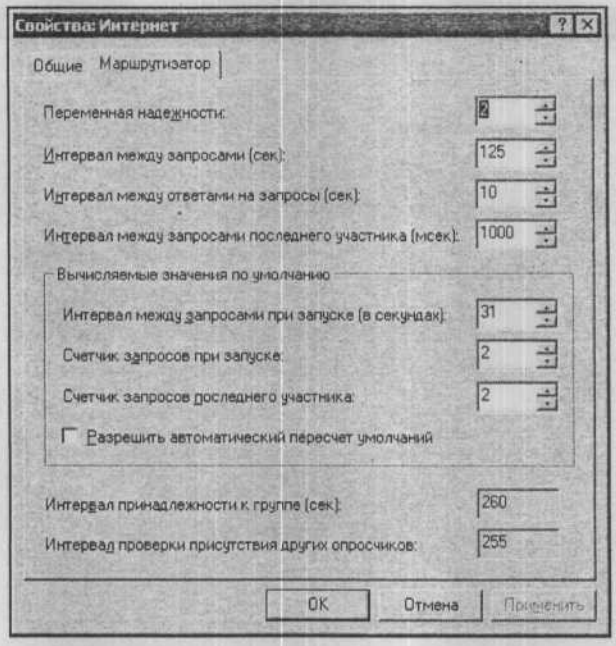

Рис. 2.41. Окно **Свойства: Интернет**, вкладка **Маршрутизатор**

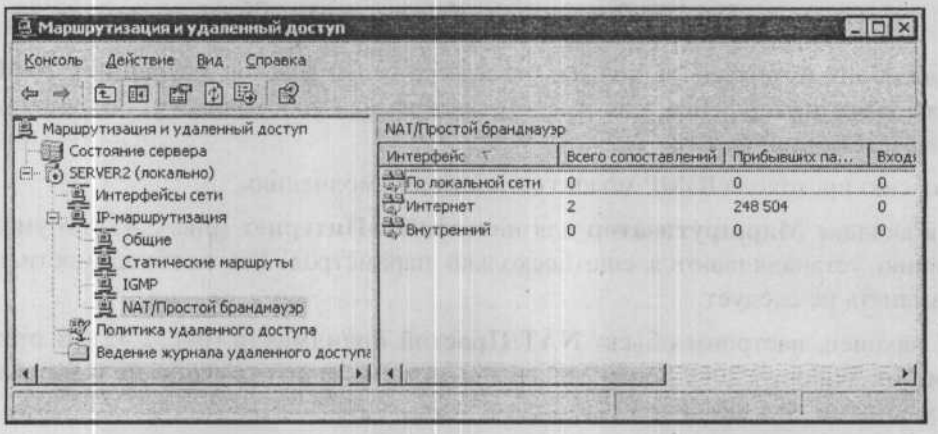

Рис. 2.42. Окно **Маршрутизация и удаленный доступ (NAT/Простой брандмауэр)**

На вкладке **Службы и порты** (рис. 2.45) необходимо выбрать или добавить порты, которые должны быть открыты со стороны Интернета в вашу сеть.

Совет

Не открывайте лишних, не применяемых по необходимости, портов. Каждый открытый порт — это окно в вашу сеть. Через эти порты в сеть могут проходить пакеты, не запрашиваемые из нее.

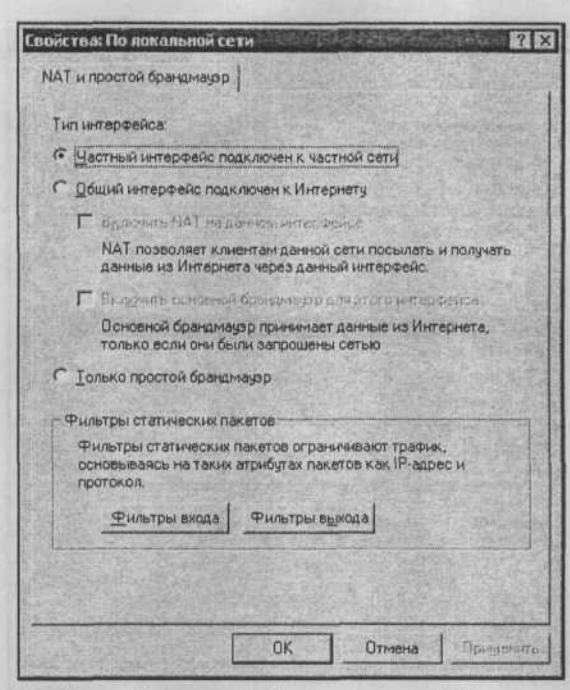

Рис. 2.43. Окно **Свойства: По локальной сети**, вкладка **NAT и простой брандмауэр**

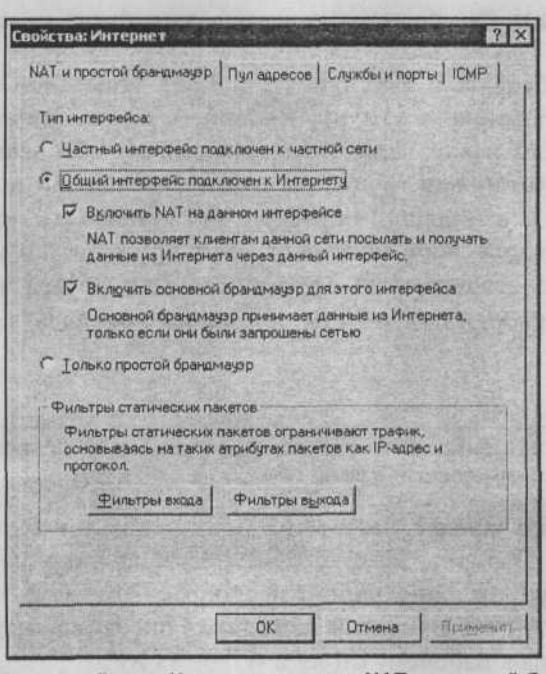

Рис. 2.44. Окно **Свойства: Интернет**, вкладка **NAT и простой брандмауэр**

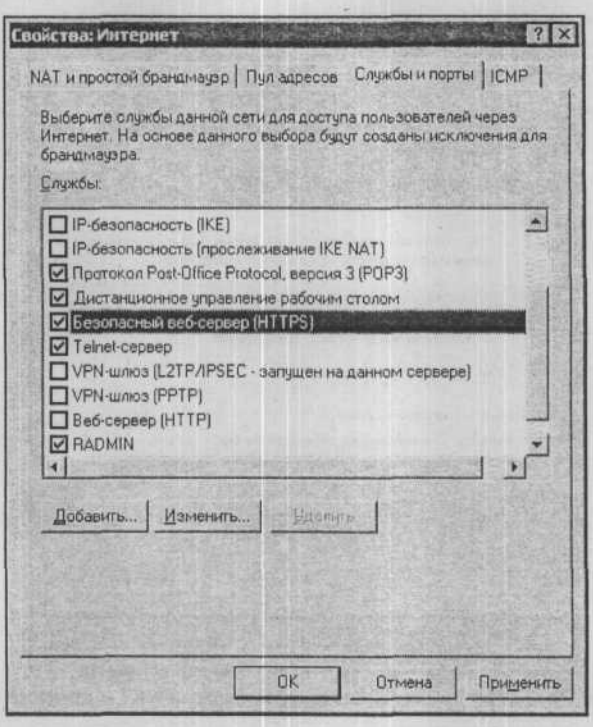

Рис. 2.45. Окно **Свойства: Интернет**, вкладка **Службы и порты**

Порты можно добавлять и изменять (рис. 2.46). Известное средство удаленного администрирования — утилиту Radmin — можно применить для управления вашей сетью извне. При этом необходимо обеспечить достаточный уровень защиты, установив трудно раскрываемые пароли и аутентификацию NTFS. Входящий и исходящий порты можно установить произвольно. Важно, чтобы исходящий порт соответствовал применяемому в вашей сети. IP-адрес должен соответствовать адресу того компьютера, на котором установлен Radmin-сервер, и при этом не обязательно совпадать с адресом интернет-сервера.

Внимание!

Применение авторизации по простому паролю может привести к несанкционированному проникновению в сеть.

Некоторые службы заранее настроены и их необходимо только включить, указав конечный IP-адрес. На рис. 2.47 показано окно настройки службы **Дистанционное управление рабочим столом**. Этот порт применяется для работы через сервер терминалов в серверных операционных системах и для удаленного доступа к рабочему столу в Windows XP.

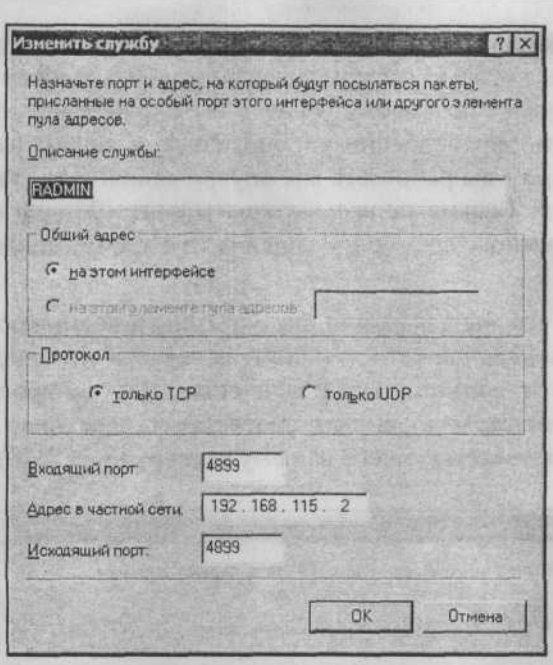

Рис. 2.46. Окно **Изменить службу (RADMIN)**

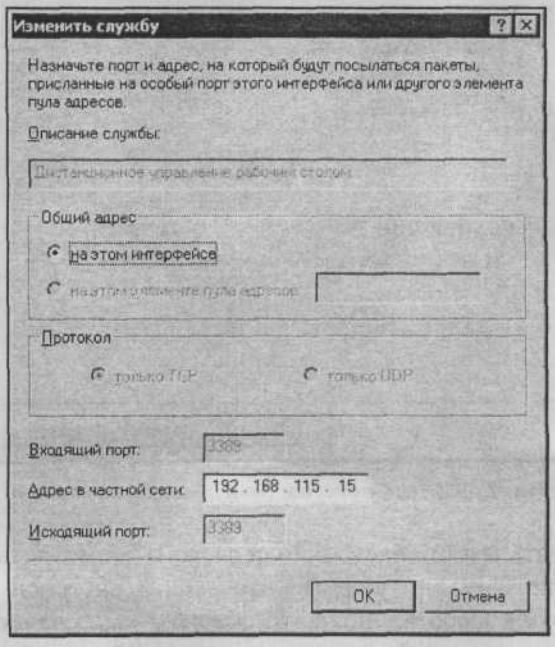

Рис. 2.47. Окно **Изменить службу (Дистанционное управление рабочим столом)**

Аналогично можно установить доступ к почтовому серверу, Web-серверу и другим службам, которые вы намерены применить в вашей сети. При этом для доступа к своему почтовому серверу вы сможете использовать внешний адрес вашей сети, что особенно удобно, когда в вашем распоряжении есть ноутбук, на котором вы работаете как внутри вашей сети, так и из дома через dial-up, например. Весьма полезно открыть порт 123 для обеспечения синхронизации системного времени в вашей сети с каким-либо сервером точного времени.

Несмотря на то, что мы настроили доступ извне и возможность подключения к Интернету из локальной сети, в свойствах сервера установлены лишь опции **маршрутизатор** и **только локальной сети**. Для контроля посмотрите на свойства интернет-сервера, вызвав соответствующее окно из контекстного меню объекта, соответствующего вашему серверу (рис. 2.48).

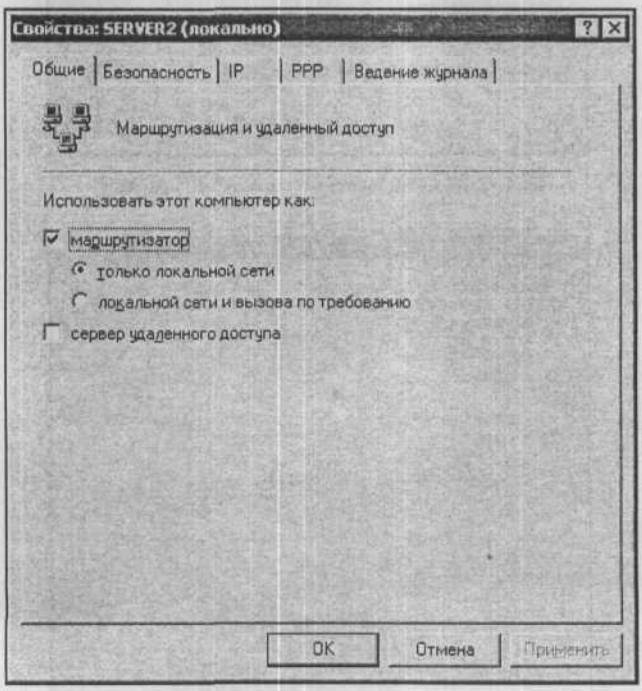

Рис. 2.48. Окно **Свойства: [имя сервера] (локально)**

Если теперь вызвать мастер настройки сервера и посмотреть его уже существующие роли (рис. 2.49), то увидим, что сервер настроен в роли **Сервера удаленного доступа**. Собственно, с этого можно было начать, и мастер установил бы начальные настройки самостоятельно. Но уточнение настроек необходимо провести вручную.

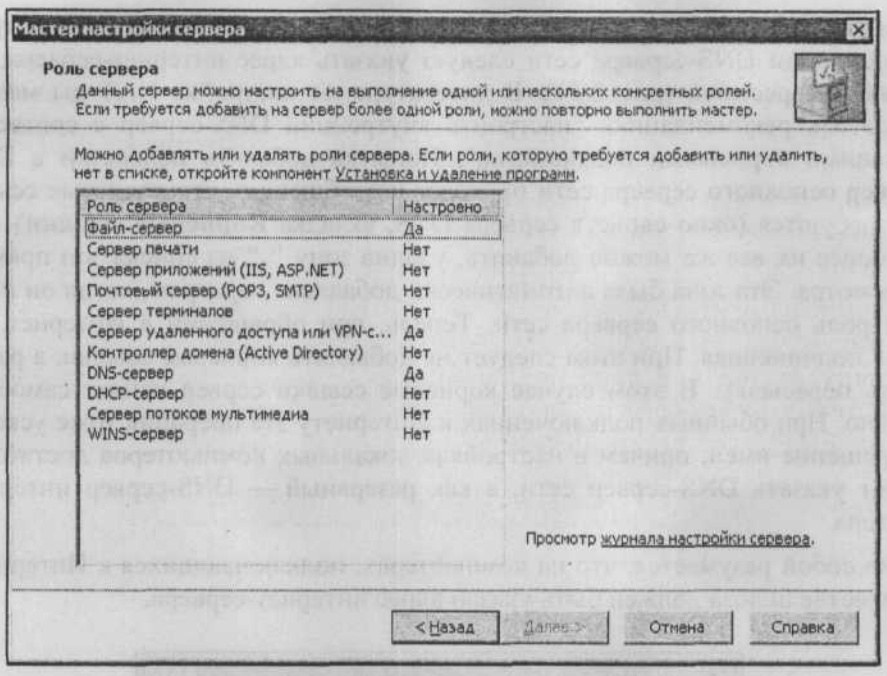

Рис. 2.49. Окно **Мастер настройки сервера (Роль сервера)**

С помощью этого же мастера можно дать еще одну роль серверу — DNS-сервер. Это не обязательно, но если, например, почтовые службы установлены на другом сервере, то для разрешения IP-адресов через DNS при отправке почты этому серверу потребуется обращаться к внешним DNS-серверам. Для того чтобы это было возможно, необходимо интернет-сервер настроить на пересылку DNS-запросов (рис. 2.50).

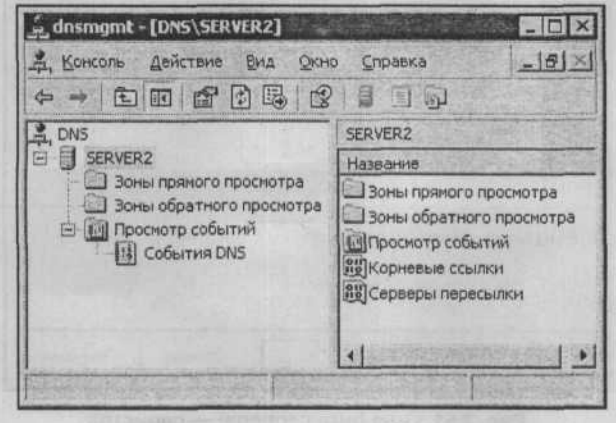

Рис. 2.50. Окно **dnsmgmt – [DNS\имя сервера]**

При этом не надо создавать никаких зон прямого или обратного просмотра, а на основном DNS-сервере сети следует указать адрес интернет-сервера, как сервера пересылки (рис. 2.51). В литературе по настройке NAT вы можете встретить рекомендацию: "настроить внутренний DNS-сервер с соответствующими корневыми подсказками". Попытка добавить подсказки в DNS-сервер основного сервера сети приведет к сообщению, что корневые ссылки не требуются (окно свойств сервера DNS, вкладка **Корневые ссылки**). Тем не менее их все же можно добавить, удалив зону "." из списка зон прямого просмотра. Эта зона была автоматически добавлена сервером, когда он получил роль основного сервера сети. Теперь, при обращении в Интернет, его роль подчиненная. При этом следует не добавлять корневые ссылки, а разрешить пересылку. В этом случае корневые ссылки сервер найдет самостоятельно. При обычных подключениях к Интернету эта операция тоже ускорит разрешение имен, причем в настройках локальных компьютеров достаточно будет указать DNS-сервер сети, а как резервный — DNS-сервер интернет-сервера.

Само собой разумеется, что на компьютерах, подключающихся к Интернету, в качестве шлюза должен быть указан адрес интернет-сервера.

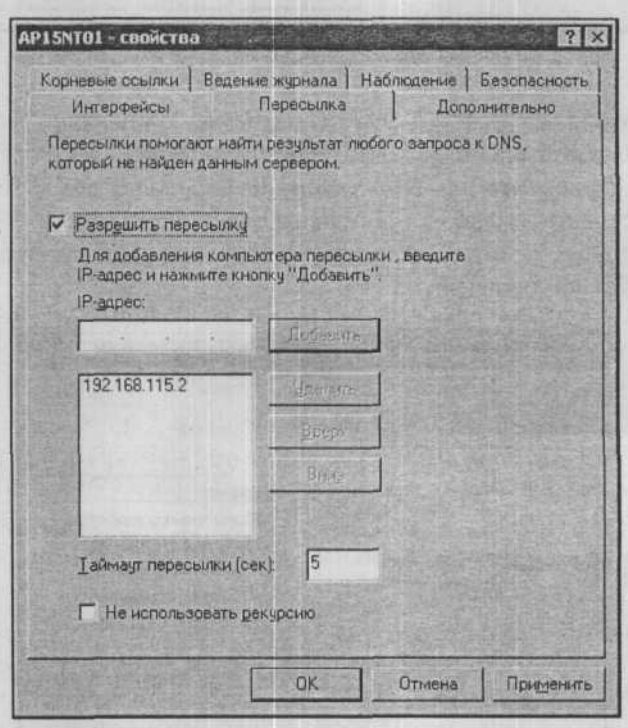

Рис. 2.51. Окно **[имя сервера] — свойства**
(Добавление адресов DNS-серверов пересылки для основного DNS-сервера)

Более подробно о настройках службы DNS можно прочитать в статье "Настройка службы DNS для подключения к Интернету на компьютере под управлением Windows 2000" в Базе знаний Microsoft по адресу:

http://support.microsoft.com/default.aspx?scid=kb;ru;300202&FR=1&PA=1&SD=HSCH.

Подключение через прокси-сервер

Подключение к Интернету с использованием NAT позволяет достаточно гибко настраивать свойства этого подключения. Но иногда вполне приемлемо более простое решение, но требующее применения дополнительных программ. Одна из таких программ — SmallProxy, которую можно бесплатно загрузить с сайта **http://www.smallproxy.narod.ru**. Автор предлагает ее, как средство для экономии трафика и ускорения работы Интернета. Она может быть применена на локальном компьютере, подключенном к Интернету, но возможности ее существенно шире. Это настоящий HTTP прокси-сервер. Через него не удастся отправлять и принимать электронную почту или работать по защищенным протоколам. Но в локальной сети часто требуется лишь обычный доступ к Web-страницам. Кроме того, предоставив возможность доступа к Интернету через описываемый прокси-сервер, вы можете без лишних сложностей контролировать трафик, используемый каждым подключением, задавать лимит трафика, разрешать и запрещать подключение для выбранных пользователей. В обычном состоянии окно программы свернуто в системном лотке и при подключении пользователя к Интернету включается анимация ее значка. Кэшируя DNS, программа позволяет ускорить доступ к уже посещенным ранее узлам и снизить трафик за счет исключения необходимости обращения к DNS-серверам. Программа сохраняет уже просмотренные страницы в своем кэше, что снижает трафик при повторном просмотре страниц другими пользователями. Кроме того, вы можете запретить посещение определенных ресурсов Интернета, ограничить показ баннеров, что также резко увеличит экономию трафика.

Предоставление доступа к Интернету через прокси-сервер не требует назначения фиксированного IP-адреса рабочим станциям. Это позволяет уменьшить число компьютеров в сети, за назначением и соблюдением уникальности IP-адресов которых вам придется следить самостоятельно.

Описанные выше настройки NAT не теряют своей ценности и необходимости, поскольку подключение через прокси-сервер следует рассматривать как дополнительную возможность. Тем не менее, если необходимо очень оперативно предоставить пользователям сети доступ к Всемирной паутине, а настройки NAT еще не выполнены, то SmallProxy позволит решить эту задачу за несколько минут. На рис. 2.52 показано окно настроек программы.

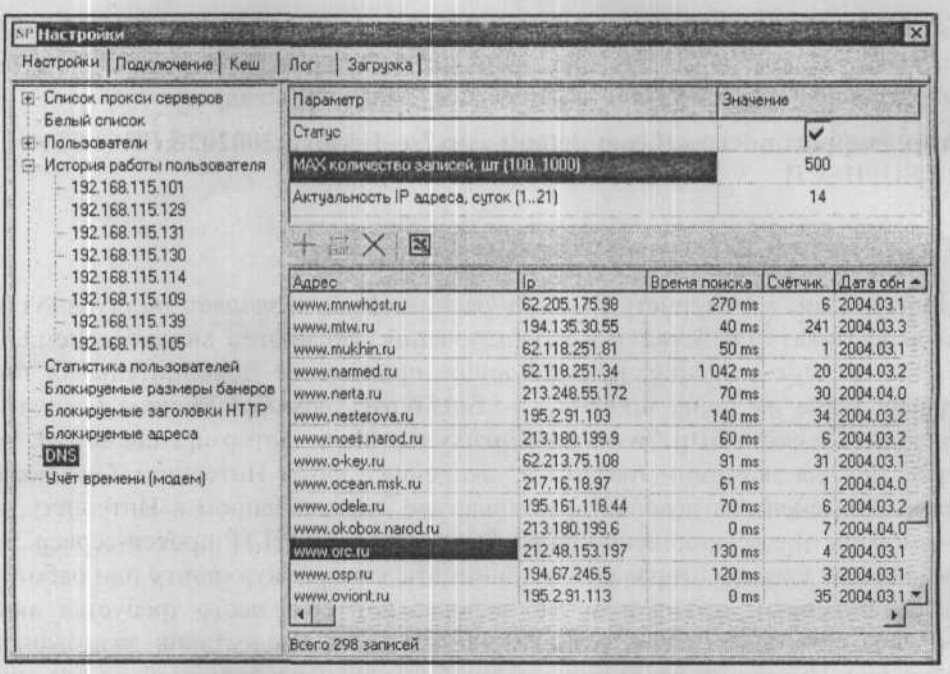

Рис. 2.52. Окно **Настройки** программы SmallProxy

Установка и настройка этой программы чрезвычайно проста. При попытке подключения к Интернету нового пользователя его учетная запись создается автоматически, но подключение для него запрещено. Вам останется разрешить или не разрешить пользователю подключение и настроить при необходимости лимит трафика.

Есть возможность и независимо от IP-адреса назначать имена и пароли пользователям. При этом необходимо установить требование авторизации для всех. Возможно, что вы найдете недостатки в этой программе, но она развивается, регулярно появляются новые версии, а бесплатной альтернативы мне обнаружить не удалось.

Мы рассмотрели основные возможности управления сервером и сервисами, предоставляемыми пользователям локальной сети. Отдельные возможности сервера будут представлены в других главах. Так например, Web-сервер, который может быть одним из сервисов, в то же время является одним из ресурсов сети, доступ к которому должен быть управляемым. Он будет рассмотрен в *главе 4*.

ГЛАВА 3

Управление файловой системой и учетными записями в сети

Один из способов управления компьютерами сети состоит в том, чтобы подключиться к удаленному компьютеру через консоль **Computer Management** (Управление компьютером). Если позволяют политики доступа к ресурсам компьютеров в вашей сети, вы можете с помощью этого средства выполнять многие операции с файлами и папками. Еще одно средство для непосредственного выполнения операций с файлами — это протокол Telnet. Для того чтобы работа через Telnet была возможна, на компьютерах, к которым предполагается подключение, необходимо запустить службу Telnet. Кроме того, для удаленного подключения к компьютеру необходимо быть членом группы пользователей Telnet на этом компьютере, а для неограниченного доступа к файлам и папкам — его администратором. Самый простой путь для обеспечения этих условий — на каждой локальной машине включить в группу администраторов компьютера администратора домена. Обычно это происходит автоматически в момент подключения компьютера к домену. Подходят и обычные средства работы с файлами, если вы имеете соответствующие разрешения на доступ к файлам и папкам удаленного компьютера по сети. Также возможно применение сценариев и программ, подготовленных администратором для осуществления необходимых процедур. Рассмотрим примеры выполнения операций на компьютерах сети с использованием различных средств, применение которых может быть более или менее удобным в зависимости от конкретной ситуации. При описании примеров нам придется обращаться сразу к нескольким инструментам, как обычно и происходит в реальной работе администратора. Так, рассматривая средства поиска файлов, например, необходимо будет обсудить и процедуру создания общих ресурсов на удаленной машине. Если для этой "дополнительной" процедуры потребуется более детальное рассмотрение, оно будет проведено в соответствующих главах книги.

Работа с файловой системой

Одна из распространенных задач администратора сети — управление файлами на рабочих станциях и сервере. Возникает она в связи с обслуживанием компьютеров, установкой или удалением программ, оказанием помощи пользователям и во многих других случаях. Выполняться такая задача может как локально, так и с доступом к компьютеру из сети.

Поиск файлов

Не надо объяснять, зачем нужна такая операция. Случай редкий, но когда необходимо найти файл, расположенный на одном из компьютеров сети, может потребоваться очень продолжительное время. Проводя поиск со своего рабочего места, администратор может сократить это время, причем довольно существенно. Осуществлять поиск можно различными средствами, доступными в операционной системе. С поиском файлов на локальной машине знакомы все. Те же средства можно применить для поиска файлов в сети, на других компьютерах, но для этого необходимо иметь права для подключения к компьютеру через сеть. Со своей рабочей станции следует зарегистрироваться в сети с правами администратора домена. Это позволит, подключившись к удаленному компьютеру, создать на нем общие ресурсы, в которых можно будет осуществлять поиск, подключив эти ресурсы к своему компьютеру как сетевые диски.

Последовательность действий для поиска файлов на удаленной машине состоит из следующих шагов:

1. Откройте оснастку **Управление компьютером**.
2. В появившемся окне **Computer Management** в пункте меню **Действие** выберите **Подключиться к другому компьютеру**.
3. В окне **Выбор компьютера** можно ввести IP-адрес компьютера или с помощью кнопки **Обзор** открыть окно **Выбор: Компьютер** и найти требуемую машину.
4. Нажать **OK** в этом и следующем окне.
5. В окне **Выбор компьютера** после поиска компьютера появится его полное имя, нажмите **OK**, если выбор верен.

   Теперь в окне **Computer Management** вы увидите консоль управления удаленным компьютером, имя которого указано рядом со значком компьютера в левой части окна (рис. 3.1).
6. Щелкните на папке **Общие ресурсы** в левой части окна, в правой части вы увидите список общих ресурсов.

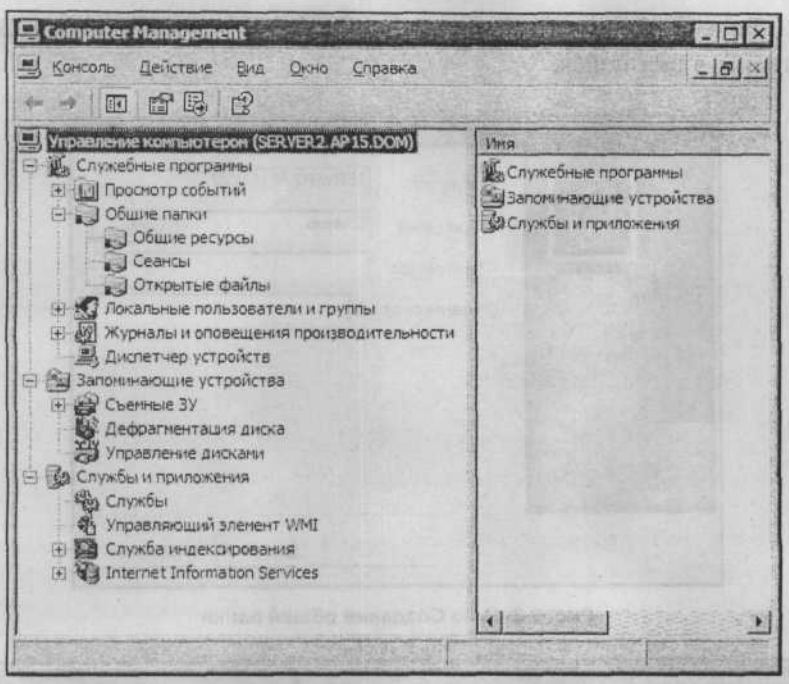

Рис. 3.1. Окно **Computer Management**

7. Щелкните правой кнопкой мыши на папке **Общие ресурсы** в левой части окна. Выберите **Новый общий ресурс**. В открывшемся окне **Создание общей папки** введите имя папки, в которой вы намерены осуществить поиск (рис. 3.2). Если вы не помните имя, то с помощью кнопки **Обзор** выберите в дереве папок необходимое и нажмите **OK**.
8. Введите имя общего ресурса и его описание, нажмите кнопку **Далее**.
9. В следующем окне выберите необходимый тип доступа и нажмите **Далее**.
10. Если не требуется еще один общий ресурс, откажитесь от его создания.

На следующем рисунке (рис. 3.3) можно видеть только что созданный общий ресурс **Дистрибутивы** на компьютере Server2.AP15.DOM. Если вы установили права на этот ресурс только для администратора, то в дальнейшем его можно использовать повторно, не опасаясь несанкционированного доступа. Если допустимо, то можно установить необходимые права на этот ресурс и для других пользователей.

Теперь достаточно найти этот ресурс в сетевом окружении и подключить на своем компьютере в качестве сетевого диска. С этого момента поиск файлов на нем возможен обычными средствами Windows. При необходимости можно

создать общие ресурсы, доступные администратору на всех машинах сети и осуществлять в них поиск.

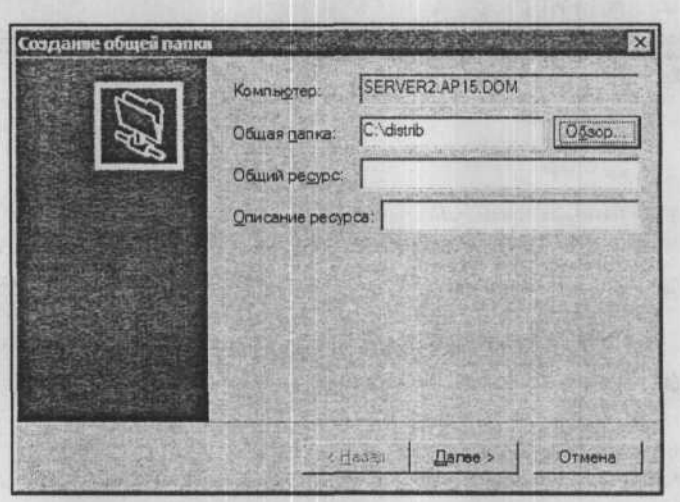

Рис. 3.2. Окно **Создание общей папки**

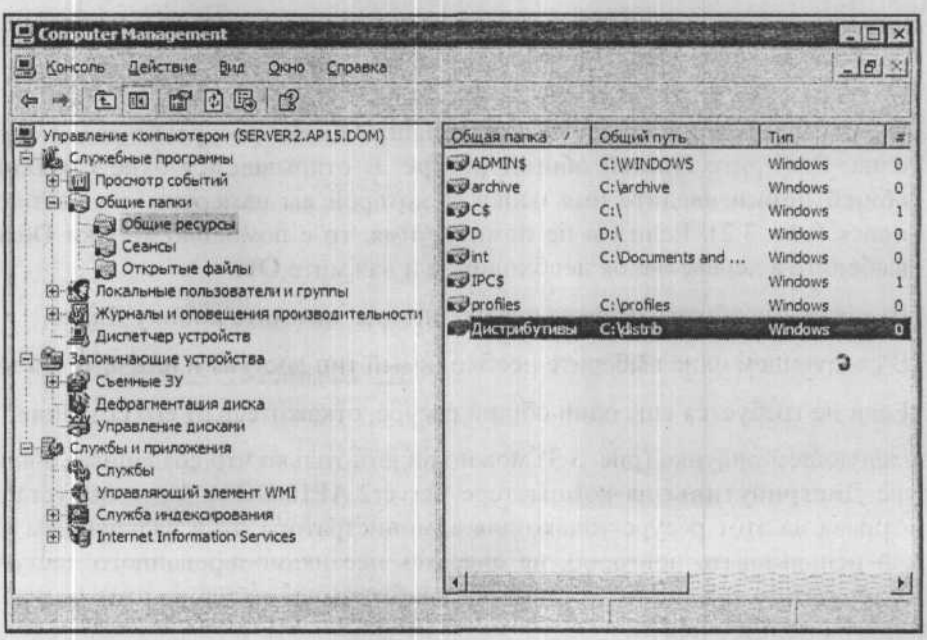

Рис. 3.3. Окно **Computer Management** с созданным новым общим ресурсом

Окно **Computer Management** (Управление компьютером), которое мы применили для поиска файлов, может использоваться в самых различных задачах

администрирования. Уже сейчас, готовя плацдарм для поиска файлов, нами был создан общий ресурс, а это тоже одна из задач, часто встречающаяся в практике администратора.

Мы еще не раз обратимся к этому средству, а теперь рассмотрим еще один путь поиска файлов в сети — Telnet.

Telnet

Если вы не уверены, что на удаленной машине запущена служба Telnet и установлены соответствующие права для вас, можно воспользоваться уже знакомым нам средством **Computer Management** (Управление компьютером) для запуска этой службы на удаленной машине. В открытом и подключенном к выбранному компьютеру окне **Computer Management** разверните **Службы и приложения** в левой части окна и выделите **Службы**. В правой части окна вы увидите список служб, найдите среди них службу **Telnet** и запустите ее. Предварительно необходимо внести свою учетную запись в группу **TelnetClients** (В том же окне **Локальные пользователи и группы | Группы | TelnetClients**).

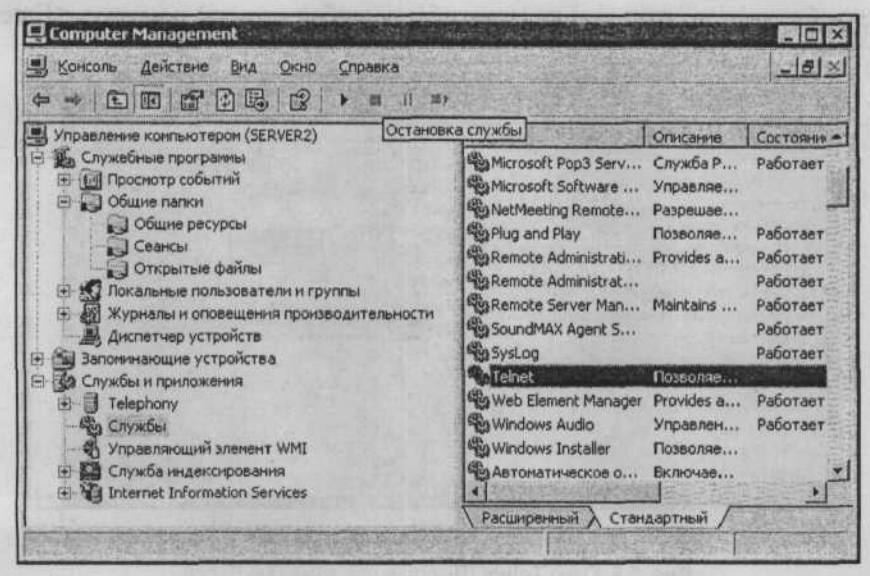

Рис. 3.4. Окно **Computer Management** служба **Telnet**

Теперь вы имеете возможность подключения к серверу Telnet, работающему на удаленной машине. При этом вы можете выполнять практически любые команды из командной строки, в том числе и команду `Find` для поиска файлов. Применение Telnet не требует организации общего доступа к файлам и

папкам, поскольку поиск идет на локальной машине с точки зрения сервера Telnet, к которому вы подключаетесь.

Для поиска файлов на удаленной машине следует проделать следующее:

1. Выполните `Telnet`.
2. Введите в открывшемся окне клиента Telnet команду

   ```
   Open <имя_компьютера_или_IP-адрес>
   ```

3. Если вы вошли в систему под учетной записью администратора домена, то вы сразу окажетесь в корне диска C:\ на удаленной машине. Иначе появится приглашение для ввода имени пользователя (`Login:`), введите имя учетной записи администратора удаленной машины.
4. Появится приглашение для ввода пароля (`Password:`), введите пароль администратора удаленной машины. В командной строке пароль отображаться не будет. После удачного ввода учетных данных вы окажетесь в каталоге администратора удаленной машины.
5. Теперь достаточно ввести команду `Find` с параметрами, например, так:

   ```
   Find "*" <часть_имени_файла*.txt>
   ```

   ("*" обозначает, что в файле может быть любая строка) и нажать <Enter>.

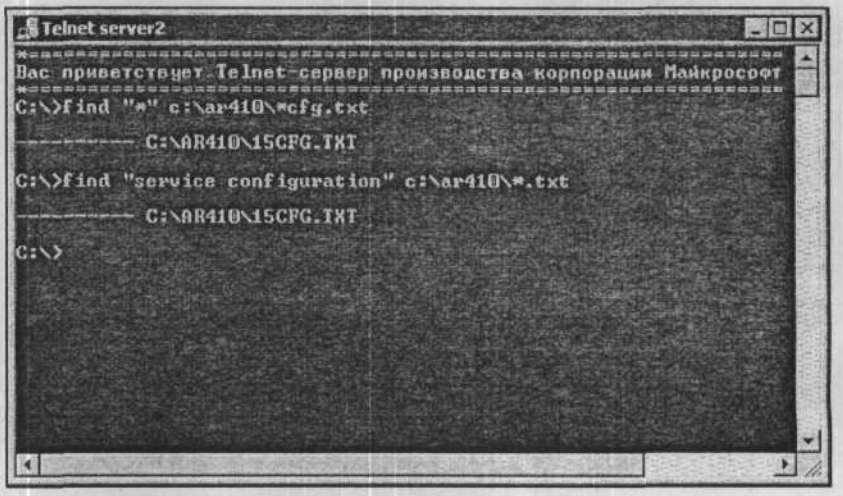

Рис. 3.5. Окно **Telnet** (Выполнение команды `Find`)

На экране появится список файлов, удовлетворяющих условиям поиска. Если это текстовый файл с кодировкой DOS, можно напечатать команду:

```
Copy <путь_имя файла> con
```

для просмотра его содержимого.

По завершении работы в сеансе введите команду `Exit` для выхода из режима командной строки, а затем `Quit` для завершения сеанса Telnet. К сожалению, из окна **Telnet** нельзя использовать программы и утилиты, имеющие графический интерфейс. Даже текстовый редактор Edit, оставшийся в составе операционных систем Windows со времен DOS, работать не будет, а все действия с файлами необходимо выполнять из командной строки без использования файловых менеджеров.

Применение сценариев

Два следующих варианта выполнения поиска файлов не слишком удобны для регулярного применения, но позволяют их использовать при автоматизации процесса поиска[1]. Для подготовки описываемых ниже средств работы с файлами необходимо некоторое знакомство со сценариями на языке JScript.

Регулярные выражения

В описываемом ниже сценарии применяются регулярные выражения, которые позволяют описать маски имен файлов для поиска, что, в свою очередь, дает возможность гибко управлять критериями поиска. Краткое описание некоторых регулярных выражений приведено ниже в табл. 3.1.

***Таблица 3.1.** Регулярные выражения*

Регулярное выражение	Описание
.	Любой отдельный символ
*	Повторение любого символа в любом количестве или нет символов
+	По крайней мере один или более предшествующих символов. Например, `ba+c` соответствует `bac`, `baac`, `baaac`, но не `bc`
^	Начало строки
$	Конец строки
[]	Любой из символов, содержащихся в скобках, или любом из диапазона символов ASCII, отделенных дефисом. Например, `b [aeiou] d` соответствует `bad`, `bed`, `bid`, `bod` и `bud`, и `r [eo] +d` — `red`, `rod`,`reed` и `rood`, но не `reod` или `roed`. `x [0-9]` соответствует `x0`, `x1`, `x2` и т. д. Если первый символ в скобках " ^ ", то регулярное выражение соответствует любым символам, кроме тех, что в скобках

[1] Мы уже рассматривали автоматизацию обслуживания базы данных и автоматизированную отправку почтовых сообщений. Автоматизация любых других процедур может потребоваться при решении тех или иных задач, возникающих перед администратором сети.

Таблица 3.1 (окончание)

Регулярное выражение	Описание
[^]	Любой символ кроме тех, что после символа " ^ " в скобках, или входящих в диапазон символов ASCII, отделенных дефисом. Например, x [^0-9] соответствует xa, xb, xc и т. д., но не x0, x1, x2 и т. д.
\	Отменяет действие специальных символов, перечисленных выше. Например, 100$ соответствует 100 в конце строки, но 100\$ соответствует набору символов 100$ в любом месте строки

В сценарии (листинг 3.1) использовано выражение "^[Д].*[t]\.doc$","i", которое соответствует имени doc-файла, начинающемуся на "Д" и оканчивающемуся буквой "t".

Листинг 3.1. Сценарий FindFls.js

```
/*******************************************/
/* Имя: FindFls.js                         */
/* Язык: JScript                           */
/* Описание: Поиск файлов                  */
/*******************************************/
// Объявляем переменные
var WshShell,FSO,Folder,ColFind,RegExp,SFileNames;

// Функция для поиска файлов в заданном каталоге
function FindFiles(Fold,RegEx) {
  var Files,SName; // Объявляем переменные
  ColFind=0; // Счетчик найденных файлов
  SFileNames=""; // Строка с именами файлов
  // Создаем коллекцию файлов в каталоге Fold
  Files=new Enumerator(Fold.Files);
  // Цикл по всем файлам в коллекции
  while (!Files.atEnd()) {
    // Выделяем имя файла
    SName=Files.item().Name;
    // Проверяем, соответствует ли имя файла регулярному
    // выражению
    if (RegEx.test(SName)) {
      ColFind++; // Увеличиваем счетчик найденных файлов
      // Добавляем имя файла к переменной SFileNames
      SFileNames+=SName+"\n";
      }
```

```
    Files.moveNext(); // Переходим к следующему файлу
    }
  SItog="Найдено файлов: "+ColFind;
  // Выводим на экран имена и количество найденных файлов
  WScript.Echo(SFileNames+SItog);
  }

/******************  Начало  *********************************/
// Создаем объект WshShell
WshShell=WScript.CreateObject("WScript.Shell");
// Создаем объект FileSystemObject
FSO=WScript.CreateObject("Scripting.FileSystemObject");
// Создаем объект Folder для доступа к подкаталогу Новая папка
// текущего каталога
Folder = FSO.GetFolder(WshShell.CurrentDirectory+"\\Новая папка");
// Создаем регулярное выражение
RegExp=new RegExp ("^[д].*[t]\.doc$","i");
// Ищем файлы с расширением .doc, имена которых начинаются на "д"
// и заканчиваются на "t"
// в каталоге Folder\Новая папка
// Флаг "i" – поиск без учета регистра
FindFiles(Folder,RegExp);

/*************  Конец ***********************************************/
```

Результат выполнения сценария будет показан на экране. Файл сценария должен быть помещен вне папки поиска. Данный сценарий без изменений может быть использован только на локальном компьютере.

Сценарий отображения всех файлов в папке

В листинге 3.2 приведен сценарий для вывода всех файлов, содержащихся в папке.

Листинг 3.2. Скрипт FlsAll.js

```
/*********************************************************************/
/* Имя: FlsAll.js                                                    */
/* Язык: JScript                                                     */
/* Описание: Получение списка всех файлов заданного каталога         */
/*********************************************************************/
// Объявляем переменные
var FSO,F,Files,WshShell,PathList,s;
```

```
// Создаем объект FileSystemObject
FSO=WScript.CreateObject("Scripting.FileSystemObject");
// Создаем объект WshShell
WshShell=WScript.CreateObject("Wscript.Shell");
// Определяем путь к папке "Новая папка"
PathList = FSO.GetFolder(WshShell.CurrentDirectory+"\\Новая папка")+ "\\"
// Создаем объект Folder (F) для папки "Новая папка"
F=FSO.GetFolder(PathList);
// Создаем коллекцию файлов каталога "Новая папка"
Files=new Enumerator(F.Files);
s = "Файлы из каталога "+PathList+"\r"+"\n";
// Цикл по всем файлам
for (; !Files.atEnd(); Files.moveNext())
  // Добавляем строку с именем файла
  s+=Files.item().Name+"\r"+"\n";
// Выводим полученные строки на экран
WScript.Echo(s);
// Создаем log-файл в папке "Мои документы"
WshShell=WScript.CreateObject("Wscript.Shell");
WshFldrs=WshShell.SpecialFolders;
PathListDoc=WshFldrs.item("MyDocuments")+"\\";
flog=FSO.OpenTextFile(PathListDoc+"FlsAll.txt",2,true)
flog.WriteLine(s);
/************  Конец ******************************************/
```

Результат работы этого скрипта будет показан на экране и выведен в файл Мои документы \ FlsAll.txt. Файл скрипта должен быть помещен вне папки поиска.

Вы можете модифицировать эти сценарии, используя некоторые особенности каждого из них. Так, в последнем применяется объект SpecialFoders, позволяющий обратиться к специальным папкам Windows и не указывать пути к ним. Кроме того, в последнем сценарии информация выводится не только на экран, но и в файл. При дальнейшей модификации допускается выводить информацию в переменную или в массив, содержание которого может быть проанализировано, а информация о результате анализа использована для генерации сигнала администратору, другому сценарию или программе. Такой сценарий может быть запущен на удаленной машине, а результат его работы использован в программных средствах автоматизации. Постепенно, рассматривая новые примеры, мы будем усложнять задачи, добавляя новые возможности.

Далее рассмотрим работу как с файлами, так и с каталогами. Администрирование сети нередко требует создания, удаления, изменения атрибутов не только файлов, но и каталогов, содержащих эти файлы.

Создание, удаление и изменение файлов и каталогов

Такие задачи могут возникать в самых различных ситуациях. Одна из часто встречающихся задач — это создание различных файлов отчетов и log-файлов, разместить которые желательно в отдельном каталоге, а после их накопления хотелось бы удалить устаревшие. Вариант создания лог-файла посредством сценария мы уже обсудили в предыдущем примере, поэтому коротко рассмотрим варианты выполнения задачи и дополним ее другими функциями.

Создание файлов

Наиболее часто встречается задача создания текстовых файлов. Это либо лог-файлы, либо иные информационные файлы, необходимые самому администратору.

Вариант 1

Если есть необходимость создать текстовый файл на удаленной машине, а содержание внести вручную, то можно воспользоваться подключенным сетевым диском. При этом файл создается обычными средствами Windows.

Вариант 2

Если по каким-либо причинам диск подключать не следует, то файл может быть создан через Telnet. Подключившись к удаленной машине и перейдя в требуемый каталог командой `CD`, достаточно ввести следующую строку:

```
COPY CON <ИМЯ_ФАЙЛА>
```

и нажать клавишу <Enter>. После этого можно набирать требуемый текст и, закончив набор текста, нажать клавишу <F6>. Текст, набранный на экране вашего компьютера, будет сохранен в файле на удаленной машине.

Вариант 3

Снова обратимся к JScript. В этом сценарии (листинг 3.3) приведен сетевой путь к файлу. При наличии соответствующих разрешений скрипт может быть выполнен на вашей локальной машине, но файл будет создан на удаленном компьютере.

Листинг 3.3. Создание файла, запись и чтение информации

```
/*********************************************************************/
/* Имя: TextFile.js                                                  */
```

```
/* Язык: JScript                                                    */
/* Описание: Работа с текстовым файлом
/*(создание файла, запись и чтение информации)                     */
/*******************************************************************/
var FSO,F,s,adr,str1,str2,str3;  // Объявляем переменные
var ForReading = 1; // Инициализируем константы
// Значение следующей переменной измените согласно параметрам
// своей задачи – \\\\<имя_компьютера>\\<доступный_ресурс>\\<имя_файла>
adr="\\\\AP15NT01\\ASU15\\TestFile.txt"
str1=""
str2="первая строка"
str3="Строка №3"
// Создаем объект FileSystemObject
FSO=WScript.CreateObject("Scripting.FileSystemObject");
// Создаем на диске C: текстовый файл TestFile.txt
F=FSO.CreateTextFile(adr, true);
// Записываем в файл первую строку
F.Write("Это ");
F.WriteLine(str2);
// Записываем в файл пустую строку
F.WriteBlankLines(1);
// Записываем в файл третью строку
F.WriteLine(str3);
// Закрываем файл
F.Close();
// Открываем файл для чтения
F=FSO.OpenTextFile(adr, ForReading);
// Пропускаем в файле две первые строки
F.SkipLine();
F.SkipLine();
s="Третья строка из файла" + adr + "\n";
// Считываем из файла третью строку
s+=F.ReadLine();
// Выводим информацию на экран
WScript.Echo(s);
/************  Конец ***********************************************/
```

Вариант 4

Приведем еще один сценарий (листинг 3.4). Адреса локальные, но, как мы уже видели, их можно заменить на сетевые.

Листинг 3.4. Запись строк в текстовый файл и чтение из него

```
/*********************************************************************/
/* Имя: WriteTextFile.js                                             */
/* Язык: JScript                                                     */
/* Описание: Запись строк в текстовый файл и чтение из него          */
/*********************************************************************/
var FSO,F,TextStream,s;  // Объявляем переменные
// Инициализируем константы
var FileName = "test1.txt"

// Создаем объект FileSystemObject
FSO=WScript.CreateObject("Scripting.FileSystemObject");
// Создаем в текущем каталоге файл FileName
FSO.CreateTextFile(FileName);
// Создаем объект File для файла FileName
F=FSO.GetFile(FileName);
// Создаем объект TextStream (файл открывается для записи)
TextStream=F.OpenAsTextStream(2, -2);
// Записываем в файл строку
TextStream.WriteLine("Это первая строка");
// Закрываем файл
TextStream.Close();
// Открываем файл для чтения
TextStream=F.OpenAsTextStream(1, -2);
// Считываем строку из файла
s=TextStream.ReadLine();
// Закрываем файл
TextStream.Close();
// Отображаем строку на экране
WScript.Echo("Первая строка из файла " + FileName + ":\n\n",s);
/*************  Конец ***********************************************/
```

К сожалению, невозможно перебрать все варианты работы с текстовыми файлами, но уже из тех примеров, которые были рассмотрены, достаточно просто скомбинировать вариант, который необходим вам.

Создание и удаление каталогов

Вариант 1

Если есть необходимость создать/удалить каталог на удаленной машине, то можно воспользоваться подключенным сетевым диском, как это рассматривалось выше. При этом каталог создается/удаляется обычными средствами Windows.

Вариант 2

Если по каким-либо причинам диск подключать не следует, то каталог может быть создан через Telnet. Подключившись к удаленной машине и перейдя в требуемый каталог командами CD, достаточно ввести следующую строку:

```
MD <ИМЯ_КАТАЛОГА>
```

и нажать клавишу <Enter>.

Для удаления каталога можно применить команду RD.

Вариант 3

Еще один сценарий JScript (листинг 3.5). В этом сценарии для создания каталога приведен локальный путь (корневой каталог диска C:\), но его можно изменить на сетевой путь.

Листинг 3.5. Создание нового каталога

```
/*********************************************************************/
/* Имя: MkFld.js                                                     */
/* Язык: JScript                                                     */
/* Описание: Создание нового каталога                                */
/*********************************************************************/
// Объявляем переменные
var FSO, F, Folder;

// Создаем объект FileSystemObject
FSO=WScript.CreateObject("Scripting.FileSystemObject");
// Создаем объект Folder для корневого каталога диска C:\
F=FSO.GetFolder("C:\\");
// Создаем коллекцию подкаталогов каталога C:\Program Files
Folder=F.SubFolders;
// Создаем каталог C:\Новая папка
Folder.Add("Новая папка");
/************  Конец ***************************************************/
```

Следующий сценарий (листинг 3.6) предназначен для удаления каталогов.

Листинг 3.6. Удаление каталога

```
/*********************************************************************/
/* Имя: DelFld.js                                                    */
/* Язык: JScript                                                     */
/* Описание: Удаление каталога                                       */
/*********************************************************************/
```

```
// Объявляем переменные
var FSO, Folder, adr;
// Указываем каталог для удаления
adr="C:\\Новая папка"
// Создаем объект FileSystemObject
FSO=WScript.CreateObject("Scripting.FileSystemObject");
// Создаем объект Folder
Folder=FSO.GetFolder(adr);
// Удаляем каталог
Folder.Delete()
/************  Конец ********************************************/
```

Представляет интерес совместное применение сценариев и Telnet. Если в сценарии приведен локальный путь и отсутствуют элементы визуального оформления его работы (диалоговые и информационные окна), то его можно выполнять, используя команду `cscript <имя_скрипта>`. При этом выполняться он будет только в командной строке, а запуск его можно осуществить через Telnet! Важно лишь поместить его в какой-либо каталог удаленного компьютера. Подключившись к удаленному компьютеру через Telnet, командами `CD` переходим в требуемый каталог и набираем `cscript <имя_скрипта>`. После нажатия клавиши <Enter> скрипт будет выполнен. Для безопасного эксперимента можете использовать два сценария, приведенные выше: MkFld.js, а затем DelFld.js.

Изменение атрибутов файлов и каталогов

Обычно нечасто приходится изменять атрибуты файлов, но иногда это оказывается необходимо. Например, в какой-либо каталог записываются файлы-отчеты. Регулярно требуется отбирать новые файлы из этого каталога для изучения или передачи пользователю. В этом случае удобнее всего совместить процедуру копирования и изменения атрибута "A" файла (готов для архивирования), копия которого уже сделана. При следующем копировании будут отбираться только "свежие" файлы. Для этих целей в пакетный файл можно включить строку следующего содержания:

```
Xcopy \\<Имя_сервера>\<доступный_каталог>\L_*.ext c:\<Имя_каталога>\  /M
/d:06-05-2004
```

Весь текст пишется в одну строку.

`Xcopy` — команда копирования файлов с расширенными возможностями.

`L_*.ext` — имя файла с указанием части имени и расширения для случая, когда применяется некоторая стандартизация имен файлов-отчетов.

`/M` — параметр, определяющий, что копироваться должны только файлы с атрибутом "A", а после копирования этот атрибут снимается.

`/d:06-05-2004` — установка начальной даты создания файлов, с которой копирование начинается первый раз.

Для изменения атрибутов файлов можно применить команду `attrib`:

```
attrib [{+r|-r}] [{+a|-a}] [{+s|-s}] [{+h|-h}] [[диск:][путь][имя_файла]
[/s[/d]]
```

Параметры команды:

`+r` — установка атрибута "Только чтение".

`-r` — снятие атрибута "Только чтение".

`+a` — установка атрибута "Архивный".

`-a` — снятие атрибута "Архивный".

`+s` — установка атрибута "Системный".

`-s` — снятие атрибута "Системный".

`+h` — установка атрибута "Скрытый".

`-h` — снятие атрибута "Скрытый".

`[диск:][путь] [имя_файла]` — задание местонахождения и имени каталога, файла или набора файлов, атрибуты которых требуется просмотреть или изменить. Для обработки группы файлов допускается применение подстановочных знаков ("?" и "*") в параметре `имя_файла`.

`/s` — выполнение команды `attrib` и всех параметров командной строки для соответствующих файлов в текущем каталоге и всех его подкаталогах.

`/d` — выполнение команды `attrib` и всех параметров командной строки для каталогов.

Для работы с файлами и каталогами на удаленной машине можно использовать Telnet. Команда может быть включена в пакетный файл и выполнена также на удаленной машине.

Вспомогательные средства

Вы уже обратили внимание на то, что сценарии в большей степени похожи на программы, чем на пакетные файлы. Поэтому открою небольшой секрет. Для создания сценариев существуют среды разработки, как и для создания программ. В практике администратора, когда может потребоваться создание сценариев на различных языках, желательно иметь под рукой универсальное средство разработки. Такое средство существует, и его можно найти по адресу **http:// www.sapien.com/default.asp**. Конечно, это не единственное средство, но, на мой взгляд, самое удобное. Как и в среде Visual Basic, в среде PrimalScript, — так называется эта программа, — существует свойство за-

вершения строк, когда после ввода имени объекта появляется список свойств и методов, доступных для него.

На момент написания книги была доступна версия 3.1, на примере которой покажем работу с конкретным сценарием. Кроме среды для создания сценариев, можно применить отладчик сценариев, который входит в состав Windows 2000 Server и Windows Server 2003. Он расположен по адресу **http://www.microsoft.com/downloads**. При загрузке отладчика обратите внимание на его версию, должна быть версия Script Debugger for Windows NT 4.0, 2000, and XP.

Если вы уже установили PrimalScript, попробуем поработать с одним из готовых сценариев в этой среде.

Щелкнув правой кнопкой на файле сценария FlsAll.js, выберем в контекстном меню **Edit With PrimalScript**. Откроется окно, показанное на рис. 3.6.

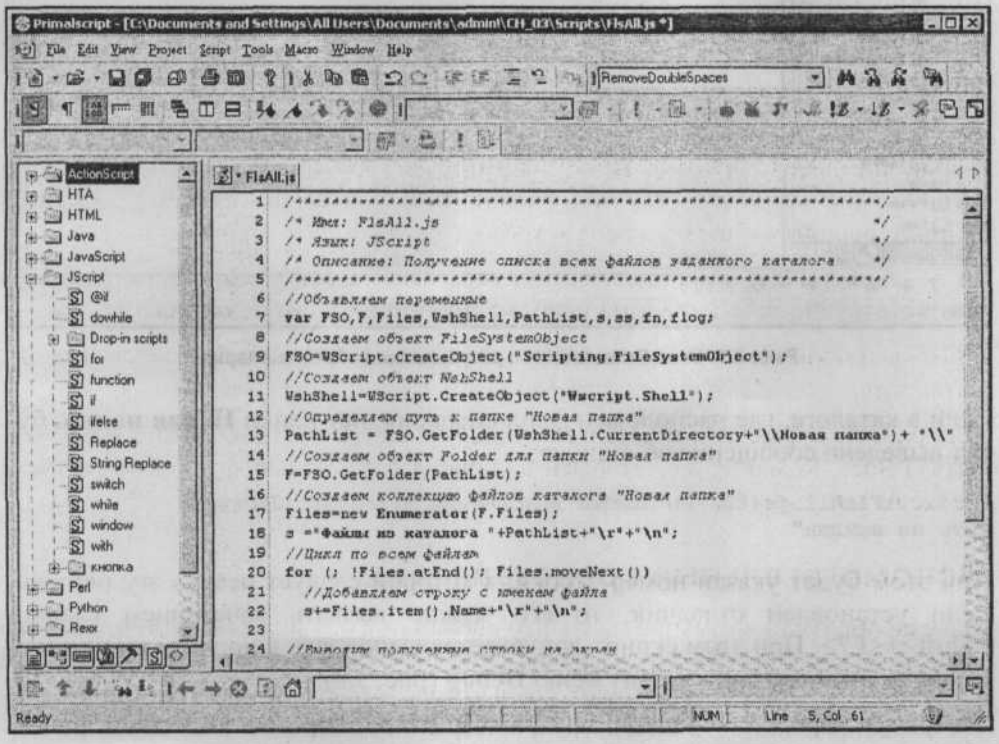

Рис. 3.6. Окно **Primalscript** с открытым файлом сценария

Чтобы сохранить исходный файл неповрежденным, создайте на диске файл с именем FlsAll2.js, переименовав новый текстовый файл, например, и сохраните открытый файл, выбрав в меню **File | Save As...**, и введя имя нового фай-

ла. Теперь нажмите клавишу <F7>. Сценарий будет выполнен, откроется новая вкладка **Output**, в окне которой разместится результат работы сценария.

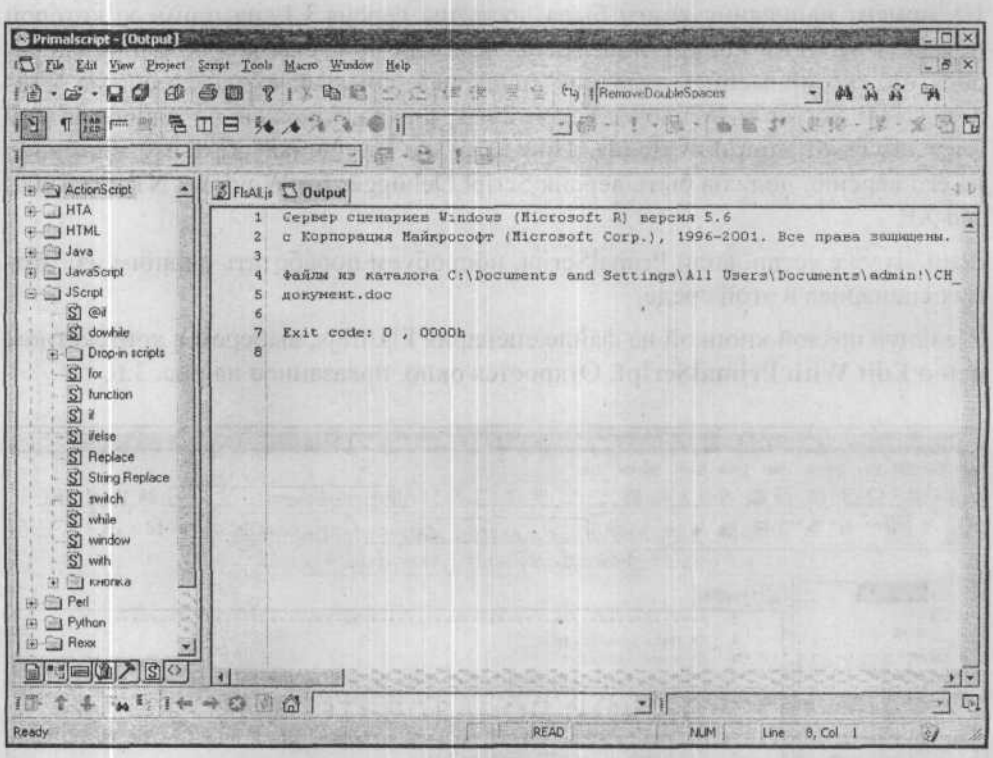

Рис. 3.7. Окно **Primalscript** с результатом работы сценария

Если в каталоге, где расположен файл сценария, нет папки **Новая папка**, будет выведено сообщение об ошибке:

```
"C:\...\FlsAll.js(13, 1) Ошибка выполнения Microsoft JScript:
Путь не найден"
```

При этом будет указан номер строки, в которой следует искать эту ошибку. Если установлен отладчик, то его можно вызвать сочетанием клавиш <Shift>+<F7>. При этом скрипт допускается выполнять в пошаговом режиме, выбирая команду `Step InTo` из меню **Debug** (рис. 3.8).

Это очень короткое описание программы PrimalScript, дающее лишь общее представление о программе. Возможностей у программы очень много, есть мастера для создания отдельных сценариев и целых проектов. Более полное описание представлено в документе **http:// www.sapien.com/tutorials /ps20minutes.pdf**. Программа будет очень полезным дополнением арсенала администратора сети, если вы предполагаете писать сценарии регулярно.

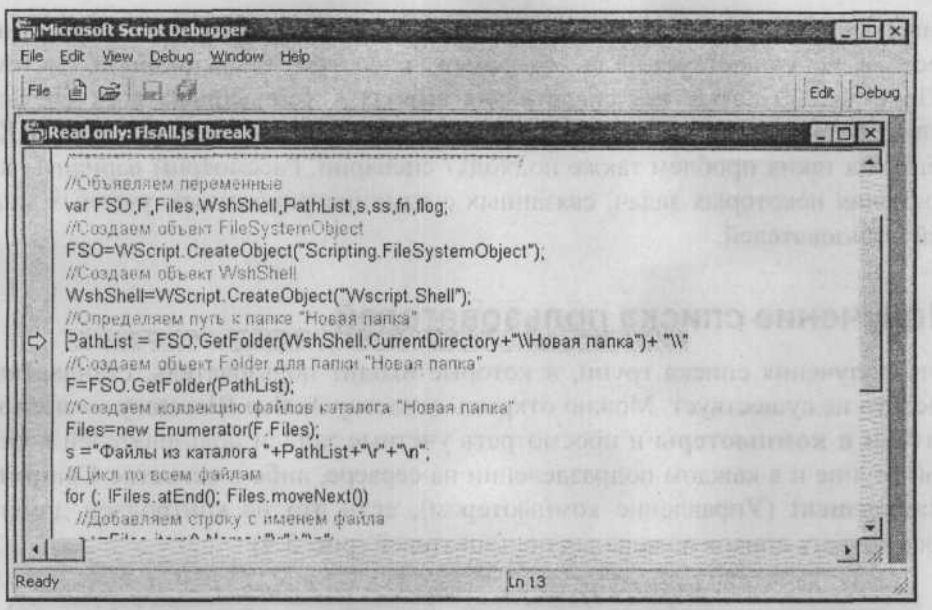

Рис. 3.8. Окно отладчика **Microsoft Script Debugger** с выделенной строкой кода, содержащей ошибку

Управление учетными записями пользователей

Одна из задач администратора сети — контроль над правильностью распределения прав пользователей сети и актуальностью их учетных записей. В связи с этим приходится просматривать учетные записи с помощью средств администрирования сервера или домена. Работа с учетными записями пользователей может быть как индивидуальной, так и массовой, когда не только просмотр, но и изменение их свойств осуществляется для значительного их числа.

Внимание!

Ошибки при изменении свойств учетных записей пользователей могут привести к серьезным проблемам в вашей сети. Рекомендуется эксперименты проводить в тестовой среде, например, установить аналог вашего сервера на отдельный компьютер или использовать виртуальный компьютер.

Технические средства для работы с учетными записями могут быть так же разнообразны, как и средства для работы с файлами. Но наиболее подходящими для ежедневной работы администратора являются обычные средства Windows и сценарии, позволяющие выполнять многие операции с учетными

записями автоматически. Для выполнения некоторых задач стандартных средств не существует. Так, например, в составе операционной системы Windows 2000 Server нет средств для вывода в файл списка всех учетных записей пользователей в соответствии с каким-либо критерием отбора. Для решения таких проблем также подходят сценарии. Рассмотрим варианты выполнения некоторых задач, связанных с администрированием учетных записей пользователей.

Получение списка пользователей

Для получения списка групп, в которые входит пользователь, стандартных средств не существует. Можно открыть оснастку **Active Directory — пользователи и компьютеры** и просмотреть учетные записи пользователей в каждой группе и в каждом подразделении на сервере, либо в оснастке **Computer Management** (Управление компьютером), если это не контроллер домена, просмотреть список локальных пользователей (рис. 3.9).

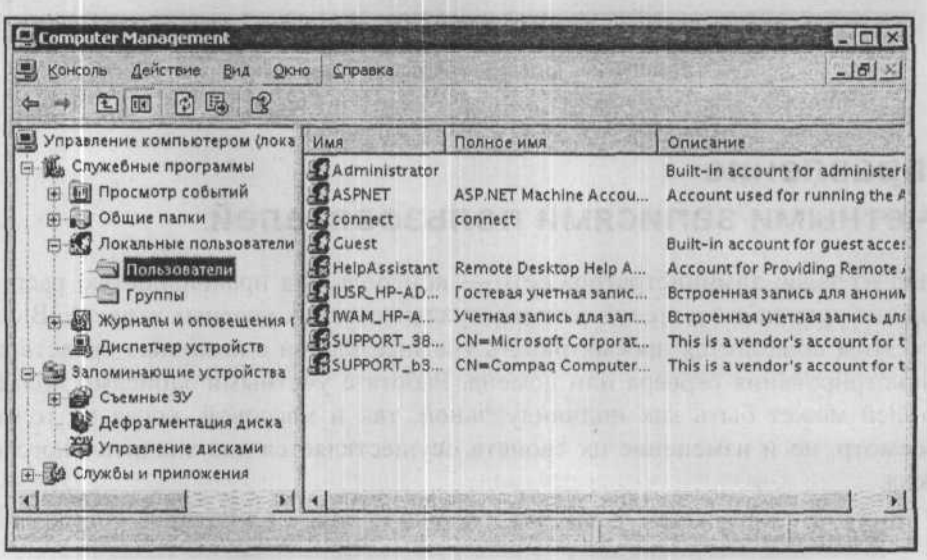

Рис. 3.9. Локальные пользователи компьютера

При общей инвентаризации пользователей вам придется провести достаточно много времени, переписывая списки пользователей. Но существуют более производительные методы работы. Правда для того, чтобы ими воспользоваться, придется провести предварительную подготовку, но когда все выполнено, можно наслаждаться плодами своего труда.

Программа на Visual Basic

Если у вас еще не установлена среда разработки Microsoft Visual Basic 6.0, то ее следует установить для выполнения следующего примера, выбрав во время установки все компоненты. Работа с мастером установки не вызовет проблем, если внимательно следовать его указаниям.

Начнем с создания нового проекта.

1. Создайте папку **User_and_Group**, в которой будет находиться наш проект.
2. Создайте новый проект на основе шаблона **Стандартный EXE**.
3. Создайте стандартный модуль.
4. Сохраните проект в созданной папке.
5. Переименуйте проект в **UsersGroups**
6. На форме **Form1** поместите два текстовых поля и в их свойствах дайте им имена **Text_Domain** и **Text_Computer**.
7. В свойстве **Text** этих полей можно записать имя домена и имя сервера, к которым вам придется обращаться наиболее часто.
8. Поместите на форме кнопку и измените ее надпись (свойство **Caption**) на **Пользователи**
9. Сохраните проект.

В результате этих действий у вас должен получиться проект, вид которого показан на рис. 3.10.

Для того чтобы работать с объектами Active Directory, необходимо подключить библиотеку **Active DS Type Library** (рис. 3.11), выбрав в меню **Проект (Project)** пункт **Информация (References)**.

Эту заготовку вы сможете использовать для создания средств работы с пользователями и группами в среде Visual Basic.

Теперь напишем код процедуры, которая будет использоваться для вывода списка пользователей. Откройте модуль **Модуль1**, выбрав его в дереве объектов проекта в окне **Проект-UserGroup** (на рис. 3.10 в этом окне видна только папка с формами), и напечатайте в нем текст, приведенный в листинге 3.7.

> ***Примечание***
>
> В вашем случае это окно может находиться в другом месте главного окна. Вы можете самостоятельно расположить его там, где будет удобно.

Сразу к возможностям нашего инструмента добавим получение сведений о полном имени пользователя и информации о его последнем входе в сеть. Не все пользователи домена или компьютера имеют полные имена и дату входа

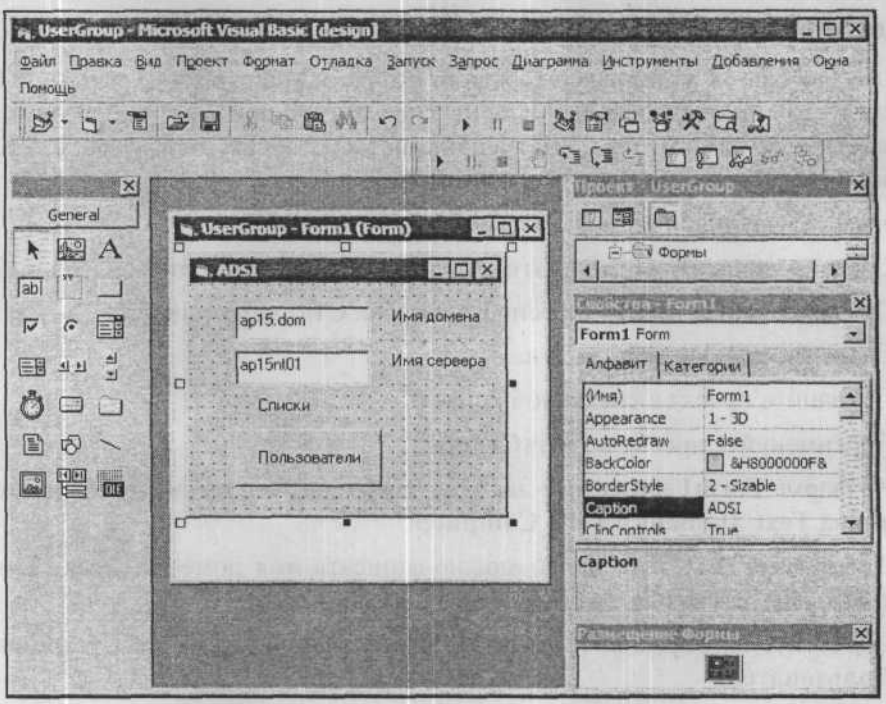

Рис. 3.10. Вид окна проекта **UserGroup**

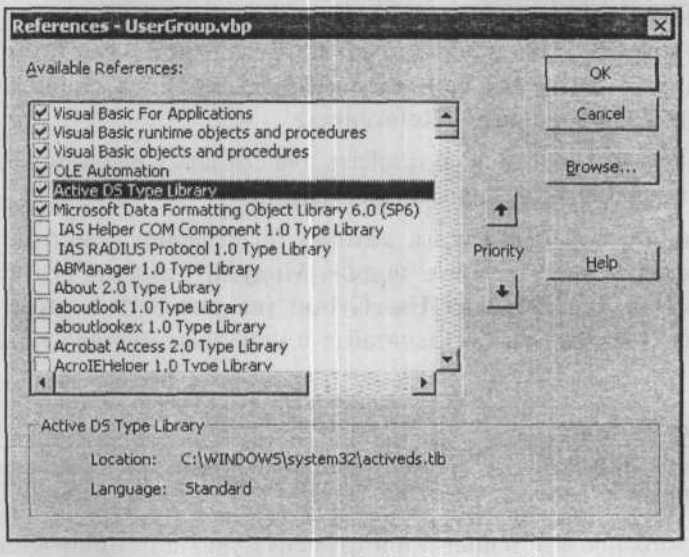

Рис. 3.11. Подключение **Active DS Type Library**

в сеть. Некоторые встроенные учетные записи никогда не использовались. Поэтому вместо даты последней регистрации в сети, при ее отсутствии, будем выводить дату "01.01.1930 00:00:00".

Листинг 3.7. Модуль1 (Public Sub userfull)

```
Option Explicit

Public Sub userfull(ComputerName As String, DomainName As String)
    Dim user As IADsUser
    Dim Container As IADsContainer
    Dim f As Integer
    Dim i As Integer
    Dim Messg As String
    Dim ScrFl As String
    Dim RetVal
       Dim ContainerName As String

        ContainerName = DomainName & "/" & ComputerName
        Set Container = GetObject("WinNT:// " & ContainerName)
        Container.Filter = Array("User")

        i = 0
        ScrFl = ""
        Messg = ""
        For Each user In Container
            i = i + 1
            On Error Resume Next
            Messg = i
            Messg = Messg & ";" & user.Name
            Err.Clear
            Messg = Messg & ";" & user.FullName
            Err.Clear
            Messg = Messg & ";" & user.LastLogin
If Err.Description <> "" Then Messg = Messg & ";" & "01.01.1930 00:00:00"
            Err.Clear
            Messg = Messg & Chr(13) & Chr(10)
            ScrFl = ScrFl & Messg
            Err.Clear
        Next

f = FreeFile
Open "c:\users.txt" For Output As f
Print #f, ScrFl
Close #f
```

```
RetVal = Shell("c:\windows\notepad.exe c:\users.txt", vbNormalFocus)
End

End Sub
```

Двойным щелчком по кнопке **Пользователи** откройте код модуля формы и в текст уже созданной автоматически процедуры `Command1_Click()` внесите строку:

```
Call Userfull (Form1.Text_Server, Form1.Text_Domain)
```

Эта строка кода позволит по нажатию кнопки вызвать процедуру, которую мы записали в **Модуль1**. При этом имена домена и сервера будут взяты из текстовых полей формы, что позволит оперативно переключаться от компьютера к компьютеру, если это необходимо.

Сохраните проект.

Если вы зарегистрированы на вашем компьютере в качестве локального пользователя, то закройте проект и запустите Visual Basic от имени администратора домена. Откройте созданный проект (при этом, возможно, снова придется подключить библиотеку **Active DS Type Library**) и запустите его на выполнение. Откроется форма, в поля которой введите имя домена и имя сервера, нажмите кнопку **OK**. Через несколько секунд будет сформирован и открыт текстовый файл c:\users.txt, в котором находится список пользователей, зарегистрированных на сервере. Список формируется с разделителями полей, поэтому его можно анализировать в MS Excell. Теперь средствами Visual Basic можно создать UsersGroups.exe и запускать его от имени администратора домена, когда требуется полный список пользователей. Когда я впервые запустил эту программу на своем компьютере, меня удивило, что в списке учетных записей были такие, о которых уже давно все забыли. Некоторые из них не использовались более года. При обычном просмотре учетных записей, когда есть более десятка групп и подразделений, обнаружить такие учетные записи довольно сложно.

Если вы заинтересуетесь созданием инструментов в среде Visual Basic, то заготовку проекта с некоторыми дополнительными функциями вы сможете скопировать с персональной страницы автора и дополнить проект своими функциями.

Получение списка пользователей с помощью сценария VBScript

Многие задачи, реализованные на Visual Basic, можно решить и с помощью VBScript. В том случае главное, что потребуется при создании нового инст-

румента, — это текстовый редактор. Создайте текстовый файл следующего содержания (листинг 3.8) и измените его расширение на vbs.

Листинг 3.8. Сценарий Users0.vbs

```
'**********Список пользователей**************
'Имя – Users0.vbs
'DomainName – введите имя домена или сервера
'Требуются права администратора домена или сервера
'Список пользователей выводится в файл Users.txt
'*********Начало процедуры*****************************************

Dim Container
Dim DomainName
Dim User
Dim StrTxt

DomainName = "ap15.dom"

Set Container = GetObject("WinNT:// " & DomainName)
Container.Filter = Array("User")
For Each User In Container
StrTxt = StrTxt & VbCrLf & User.Name

Next

'MsgBox StrTxt
set FSO = CreateObject("Scripting.FileSystemObject")
        txtlog = "Users.txt"
        set LogFile = FSO.CreateTextFile(txtlog, True)
            LogFile.WriteLine  Date & " " & Time &  vbCrLf & strtxt
        LogFile.Close
```

Вариант этого сценария с возможностью получения расширенной информации о пользователях приводится в листинге 3.9.

Листинг 3.9. Сценарий Users.vbs

```
'**********Список пользователей**************
'Имя – Users.vbs
'Включены полное имя и дата последнего входа в сеть
'DomainName – введите имя домена или сервера
'Требуются правы администратора домена или сервера
'*********Начало*****************************************
```

```
Dim Container
Dim DomainName
Dim User
Dim StrTxt
Dim Messg
Dim i

DomainName = "ap15.dom"

Set Container = GetObject("WinNT:// " & DomainName)
Container.Filter = Array("User")
 i = 0
        StrTxt = ""
        Messg = ""
        For Each User In Container
            i = i + 1
            On Error Resume Next
            Messg = i
            Messg = Messg & ";" & User.Name
            Err.Clear
            Messg = Messg & ";" & User.FullName
            Err.Clear
            Messg = Messg & ";" & User.LastLogin
If Err.Description <> "" Then Messg = Messg & ";" & "01.01.1930 00:00:00"
            Err.Clear
            Messg = Messg & VbCrLf
            StrTxt = StrTxt & Messg
            Err.Clear
        Next

'MsgBox StrTxt
set FSO = CreateObject("Scripting.FileSystemObject")
        txtlog = "Users.txt"
        set LogFile = FSO.CreateTextFile(txtlog, True)
            LogFile.WriteLine  Date & " " & Time &  vbCrLf & strtxt
        LogFile.Close
```

Списки групп и пользователей

Получение списка групп, в которые входит пользователь, и списка пользователей, которые входят в группу.

Эту задачу можно выполнить вручную, просматривая группы учетных записей и выписывая учетные записи, входящие в них. Но "Попробовав сладкого,

не захочешь горького", поэтому продолжим создание инструментов, облегчающих нашу работу.

Вариант сценария, выводящий перечень групп, приведен в листинге 3.10.

Листинг 3.10. Сценарий Groups.vbs. Список групп пользователей

```
'**********Список групп пользователей**************
'Имя — Groups.vbs
'DomainName — введите имя домена или сервера
'Требуются права администратора домена или сервера
'Сведения выводятся в файл groups.txt
'*********Начало процедуры*****************************************

Dim Container
Dim DomainName
Dim Group
Dim StrTxt

DomainName = "ap15.dom"

Set Container = GetObject("WinNT:// " & DomainName)
Container.Filter = Array("Group")
For Each Group In Container
StrTxt = StrTxt & VbCrLf & Group.Name

Next
'MsgBox StrTxt
set FSO = CreateObject("Scripting.FileSystemObject")
        txtlog = "Groups.txt"
        set LogFile = FSO.CreateTextFile(txtlog, True)
            LogFile.WriteLine  Date & " " & Time &  vbCrLf & strtxt
        LogFile.Close
'*********Конец*************************************************
```

Следующий вариант сценария (листинг 3.11) выведет полный список пользователей и групп, к которым они принадлежат. При этом в самом начале выполнения сценария можно ввести имя группы, которую хотелось бы выделить в общем перечне (с помощью восклицательных знаков по обе стороны от имени группы).

Листинг 3.11. UsersAndGroups.vbs. Список пользователей и групп, в которые они входят

```
'**********Список пользователей и групп************************
'Имя — UsersAndGroups.vbs
```

```
'DomainName – введите имя домена или сервера
'Требуются права администратора домена или сервера
'*********Начало**************************************************

ComputerName = "ap15nt01"
DomainName = "ap15.dom"
GroupName = InputBox ("Введите имя группы для выделения","Ввод
данных","Администраторы")
        ContainerName = DomainName '& "/" & ComputerName
        Set Container = GetObject("WinNT:// " & ContainerName)
        Container.Filter = Array("User")

        i = 0
        ScrFl = ""
        Messg = ""
        For Each User In Container
            i = i + 1
            'On Error Resume Next
            Messg = i
            Messg = Messg & ";" & User.Name
            'MsgBox i & " – " & User.Name
            Err.Clear
            Messg = Messg & ";" & User.FullName
            Err.Clear
 Set User = GetObject("WinNT:// " & DomainName & "/" & User.Name & ",user")

                For Each Group In User.Groups
                    If Group.Name = GroupName Then
                       Messg = Messg & ";" & "!!! " & Group.Name & " !!!"
                    Else
                       Messg = Messg & ";" & Group.Name
                    End If

                Next

            Messg = Messg & VbCrLf
            ScrFl = ScrFl & Messg
            Err.Clear
        Next

'MsgBox StrTxt
set FSO = CreateObject("Scripting.FileSystemObject")
        txtlog = "UsersAndGrops.txt"
```

```
        set LogFile = FSO.CreateTextFile(txtlog, True)
            LogFile.WriteLine  Date & " " & Time &  VbCrLf & ScrFl
        LogFile.Close
'*********Конец*************************************************************
```

Добавление учетной записи пользователя и ее разблокировка

До сих пор мы рассматривали возможности получения информации о пользователях, не пытаясь изменить что-либо в учетных записях. Но в задачах администратора не последнее место занимают процедуры добавления, изменения, удаления объектов сети, и в том числе модификации, связанные с учетными записями пользователей.

Внимание!

Даже безошибочное выполнение процедур, описанных ниже, может привести к серьезным осложнениям в вашей сети, если выполняет их не администратор.

Все сценарии и процедуры, рассмотренные выше, универсально подходят как к сети с сервером Windows NT, так и Windows 2000—2003. Уже Windows 2000 Server позволяет организовать более сложную, хотя и более гибко управляемую структуру сети, основанную на Active Directory. Многие параметры учетных записей в сети Windows 2000—2003 невозможно изменить средствами Windows NT. Кроме пользователей, компьютеров и групп, в такой сети содержатся подразделения, которые не определяют прав пользователя, но позволяют удобно организовать данные о пользователях. Подразделения могут быть вложены друг в друга. Сценарии, предназначенные для работы со структурами, входящими в новые операционные системы семейства NT, имеют некоторые отличия от тех, что были рассмотрены выше, но достаточно хорошо читаются, чтобы в них разобраться. Отличия заключаются в том, что теперь мы обращаемся не к компьютеру-серверу, а к домену, который, учитывая свойства и возможности Active Directory, уже не привязан жестко к одному компьютеру, и его имя не совпадает с именем сервера. Сценарии, приведенные далее, как и те, что рассматривались выше, полностью работоспособны, если вы измените в них имена организационных единиц (OU, Organizational unit) и имя домена на применяемые в вашей сети.

Добавление учетной записи пользователя

Сценарий, приведенный в листинге 3.12, позволяет в интерактивном режиме добавить учетную запись пользователя в Active Directory, определив основные параметры учетной записи. Перед завершением работы сценария вам будет предложено активизировать учетную запись или оставить ее заблокиро-

ванной. При вводе данных сценарий предложит значения, записанные в его тексте (значения по умолчанию), — замените их на необходимые.

Листинг 3.12. Добавление учетной записи пользователя

```
'*****************************add_users.vbs*******************************
' Добавляет пользователя в AD в OU=OKO, вложенную в OU=users и
OU=autopark
' с основными данными учетной записи
' В домене должна существовать OU (подразделение) с адресом,
' соответствующим константе sOUAddress
' Замените sOUAddress на имя ou + имя вашего домена
' В данном случае домен называется ap15.dom, OU называется "OKO"
'*************************начало*****************************************
Dim OU 'As IADs

Dim usr 'as IADsUser
Const sOUAddress = "LDAP:// OU=oko,OU=users,OU=autopark,DC=ap15,DC=dom"

        sDisplayName= InputBox _
("Введите полное имя", _
"Ввод данных нового пользователя (1из11)","Иванов Иван Иванович")
        ' Заменяем двойные пробелы на одинарные
        sDisplayName = RemoveDoubleSpaces(sDisplayName)

        ' Выделяем Фамилию, имя и отчество из sDisplayName
        iFirstSpacePos = InStr(sDisplayName," ")
        iSecondSpacePos = InStr(iFirstSpacePos+1,sDisplayName," ")
        sSurName = mid(sDisplayName,1,iFirstSpacePos-1)
        sGivenName = mid(sDisplayName,iFirstSpacePos+1, _
iSecondSpacePos-iFirstSpacePos-1)
        sMiddleName = mid(sDisplayName, _
iSecondSpacePos+1,Len(sDisplayName)-iSecondSpacePos)
        sSAMAccountName = InputBox _
          ("Введите имя для входа в сеть (login)", _
"Ввод данных нового пользователя(2из11)","zzz")
        sUserPrincipalName = sSAMAccountName & "@ap15.dom"
        sTitle = InputBox _
          ("Введите должность","Ввод данных нового пользователя
(3из11)","Программист")
        sDescription = InputBox _
          ("Введите описание","Ввод данных нового пользователя
(4из11)","abcd")
        sScriptPath = InputBox _
("Введите путь к сценарию входа","Ввод данных нового пользователя (5из11)")
```

```
        sTelephoneNumber     = InputBox _
         ("Введите телефон","Ввод данных нового пользователя
(6из11)","1234567")
        sOtherTelephone      = InputBox _
         ("Введите второй телефон","Ввод данных нового пользователя
(7из11)","123")
        sDepartment          = InputBox _
         ("Введите отдел","Ввод данных нового пользователя (8из11)","Отдел")
        sHomeDirectory       = InputBox _
         ("Введите домашний каталог","Ввод данных нового пользователя
(9из11)")
        sHomeDrive           = InputBox _
         ("Введите подключаемый диск","Ввод данных нового пользователя
(10из11)")
        sProfilePath         = InputBox _
         ("Введите профиль","Ввод данных нового пользователя (11из11)")

        Set OU = GetObject(sOUAddress)
        Set usr = OU.Create("user", "CN=" & sDisplayName)
        usr.Put "samAccountName", sSAMAccountName
        usr.Put "UserPrincipalName", sUserPrincipalName
        usr.Put "userPassword", "123456"
        usr.Put "displayName", sDisplayName
        usr.Put "sn", sSurName
        usr.Put "GivenName", sGivenName
        usr.Put "MiddleName", sMiddleName
        if not isNull(sTitle) then
               usr.Put "title", sTitle
        end if
        if not isNull(sDescription) then
               usr.Put "description", sDescription
        end if
        If (not isNull(sScriptPath) And sScriptPath <> "") then
               usr.Put "ScriptPath", sScriptPath
        end If
        If (not IsNull (stelephoneNumber)  And stelephoneNumber <> "") then
               usr.Put "telephoneNumber", stelephoneNumber
        end if
        if not isNull(sdepartment) then
               usr.Put "department", sdepartment
        end if

        If (not isNull(sHomeDirectory) And sHomeDirectory <> "") Then
               usr.Put "HomeDirectory", sHomeDirectory
        end if
```

```
        If (not isNull(sHomeDrive) And sHomeDrive <> "") Then
              usr.Put "HomeDrive", sHomeDrive
        end if
        If (not isNull(sProfilePath) And sProfilePath <> "") then
              usr.Put "ProfilePath", sProfilePath
        end If

        On Error resume Next
        usr.SetInfo
        If MsgBox("Активизировать учетную запись?", _
        vbYesNo,"Включение учетной записи")= vbYes Then
           usr.AccountDisabled = False
        usr.SetInfo
    End If
        Select Case Err.Number
              case 0
        case -2147019886 MsgBox ("Уже существует пользователь с таким
именем:" &

sDisplayName)
        case else MsgBox ("Ошибка при добавлении пользователя.
" &  Err.Number &

Err.Description)
        End Select

        Set OU = Nothing
        Set usr = Nothing
' Заменяем множественные пробелы на одинарные если таковые были введены
function RemoveDoubleSpaces(str)
        do
              str = replace(str, "  "," ")
              iDoubleSpacePos = InStr(str,"  ")
        loop while iDoubleSpacePos<>0
        RemoveDoubleSpaces = str
end Function
************************конец*****************************************
```

Создание большого числа учетных записей

Иногда возникает необходимость создать сразу несколько учетных записей для организации какой-либо специальной группы пользователей. Для подготовки такого списка лучше всего подходит приложение MS Excel, позволяющее осуществлять связь данных с другими приложениями. При запуске этого сценария необходимо зарегистрироваться в сети администратором домена и

создать источник данных Excel ODBC DSN с именем **adusers**, указывающий на файл Excel, со списком пользователей (рис. 3.12).

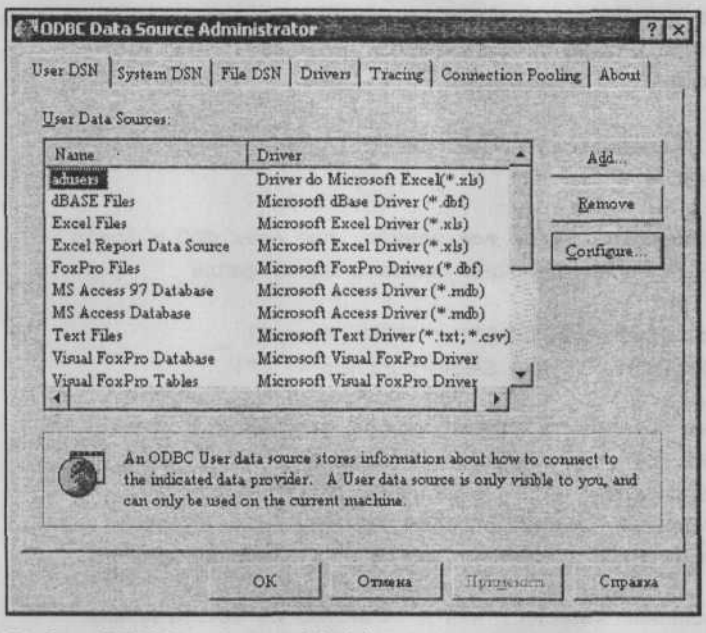

Рис. 3.12. Окно **ODBC Data Source Administrator** с созданным источником данных

Сценарий (листинг 3.13) был опубликован на одном из форумов в Интернете и приводится почти без изменений.

Листинг 3.13. Сценарий для добавления учетных записей по списку

```
'*************************************************************************
' (c) Bald
' Разумеется, можно свободно все изменять
' Добавляет пользователей с DSN 'adusers' в AD в Ou 'autopark'
' ФИО, login, отдел, профиль, login-скрипт, телефон и т. д.
' Создан на основе скрипта, опубликованного Windows 2000 Magazine
' Перед работой скрипта создайте Excel ODBC DSN с именем "adusers"
' указывающий на файл Excel, где "сидят" имена пользователей
' См. шаблон файла в архиве и примечания к полям там же
' Кроме того, в домене должна существовать OU (подразделение) с адресом,
' соответствующим константе sOUAddress
' Замените sOUAddress на имя вашего домена + имя ou
' В данном случае домен называется ap15.dom, OU называется " autopark "
'**********Начало*****************************************
```

```
On Error resume next
Const sOUAddress = "LDAP:// OU=autopark,DC=ap15,DC=dom"
Dim ou 'As IADs
Dim usr 'as IADsUser
' Открыть электронную таблицу Excel
' с помощью ADO
Dim oCN
Set oCN = CreateObject("ADODB.Connection")
oCN.Open "adusers"

' Запросом берем из Excel все записи, где есть ФИО и login
' "Новые" — название рабочего листа в Excel-файле
Dim oRS
Set oRS = oCN.Execute("SELECT * FROM [Новые$] _
where displayName<>'' and SAMAccountName<>''")

' Поочередно обработать строки набора записей
Do Until oRS.EOF
      sDisplayName        = trim(oRS("displayName"))
      ' Заменяем двойные пробелы на одинарные (функция в конце сценария)
      sDisplayName = RemoveDoubleSpaces(sDisplayName)

      ' Выделяем Фамилию, имя и отчество из sDisplayName
      iFirstSpacePos       = InStr(sDisplayName," ")
      iSecondSpacePos = InStr(iFirstSpacePos+1,sDisplayName," ")
      sSurName             = mid(sDisplayName,1,iFirstSpacePos-1)
      sGivenName _
      = mid(sDisplayName,iFirstSpacePos+1,iSecondSpacePos-
iFirstSpacePos-1)
      sMiddleName _
      = mid(sDisplayName,iSecondSpacePos+1,Len(sDisplayName)-
iSecondSpacePos)

      sSAMAccountName     = trim(oRS("SAMAccountName"))
      sUserPrincipalName  = sSAMAccountName & "@ap15.dom"
      sTitle              = oRS("title")
      sDescription        = oRS("description")
      sScriptPath         = oRS("scriptPath")
      sTelephoneNumber    = oRS("telephoneNumber")
      sOtherTelephone     = oRS("otherTelephone")
      sDepartment         = oRS("department")
      sHomeDirectory      = oRS("HomeDirectory")
      sHomeDrive          = oRS("HomeDrive")
      sProfilePath        = oRS("ProfilePath")
```

```
DsplNm = DsplNm & sDisplayName & VbCrLf
MsgBox DsplNm

   Set ou = GetObject(sOUAddress)
   Set usr = ou.Create("user", "CN=" & sDisplayName)
   usr.Put "samAccountName", sSAMAccountName
   usr.Put "UserPrincipalName", sUserPrincipalName
   usr.Put "userPassword", "123456"

   usr.Put "displayName", sDisplayName
   ' Фамилия
   usr.Put "sn", sSurName
   ' Имя
   usr.Put "GivenName", sGivenName
   ' Отчество
   usr.Put "MiddleName", sMiddleName
   if not isNull(sTitle) then
         usr.Put "title", sTitle
   end if
   if not isNull(sDescription) then
         usr.Put "description", sDescription
   end if
   if not isNull(sScriptPath) then
         usr.Put "ScriptPath", sScriptPath
   end if
   if not isNull(stelephoneNumber) then
         usr.Put "telephoneNumber", stelephoneNumber
   end if
   if not isNull(sdepartment) then
         usr.Put "department", sdepartment
   end if

   if not isNull(sHomeDirectory) then
         usr.Put "HomeDirectory", sHomeDirectory
   end if
   if not isNull(sHomeDrive) then
         usr.Put "HomeDrive", sHomeDrive
   end if
   if not isNull(sProfilePath) then
         usr.Put "ProfilePath", sProfilePath
   end if

   On Error resume next
   usr.SetInfo
```

```
        Select Case Err.Number
                case 0
        case -2147019886 MsgBox ("Уже существует пользователь с таким
именем:" & sDisplayName)
        case else MsgBox ("Ошибка при добавлении пользователя. " &
Err.Number & Err.Description)
        End SELECT
        Set ou = Nothing
        Set usr = Nothing

        ' Перейти к следующей строке набора записей.
        oRS.MoveNext
Loop
'**********************Конец*******************************************
'*****функция, заменяющая множественные пробелы на одинарные***********
function RemoveDoubleSpaces(str)
        do
                str = replace(str, "  "," ")
                iDoubleSpacePos = InStr(str,"  ")
        loop while iDoubleSpacePos<>0
        RemoveDoubleSpaces = str
end Function
'*****************************************************************************
```

Файл NewUsers.xls должен содержать лист "Новые", в котором первая строка включает имена свойств учетной записи, приведенных в тексте сценария в скобках и кавычках для объекта данных — `oRS` (например, `oRS("SAMAccountName")`). Каждая следующая строка должна содержать данные учетной записи. Во время выполнения перед добавлением каждой учетной записи на экран будет выводиться перечень обработанных учетных записей в виде полных имен пользователей. При желании, вы можете отключить эти сообщения, закомментировав строки:

```
' DsplNm = DsplNm & sDisplayName & VbCrLf
' MsgBox DsplNm
```

с помощью одинарных кавычек перед ними (как в тексте).

В табл. 3.2 приведены несколько первых полей листа. Порядок полей значения не имеет.

Все учетные записи, созданные этим сценарием, будут в заблокированном виде.

Таблица 3.2. *Лист "Новые" файла NewUsers.xls*

DisplayName	sAMAccountName	title	department	ScriptPath
Иванов Иван Иванович	Iii	Инженер	Тех.отдел	iii.bat
Петров Петр Петрович	Ppp	Юрист	Юр.отдел	ppp.bat

Удаление пользователя

Внимание!

Операция удаления объектов Active Directory необратима!

Как удалить учетную запись средствами Windows, вам известно. Напомним лишь, что эта операция требует внимания, поскольку удалить учетную запись легко, а восстановить — практически невозможно. Даже изменение пароля для некоторых учетных записей может изменить их права настолько существенно, что придется их восстанавливать заново. А удаление учетной записи администратора компьютера, а тем более домена, приведет к таким серьезным проблемам для вашей сети, что процесс восстановления ее работоспособности может занять не один день. Поэтому — осторожность и внимание!

Если при просмотре учетных записей домена не имело значения, в каком подразделении или группе находится пользователь, то для удаления учетной записи необходимо указать ее точное местоположение. Учетные записи пользователей могут находиться как внутри подразделений, созданных администратором, так и в стандартной папке пользователей Users. В примере сценария есть возможность изменить исходную точку поиска подразделений и пользователей, изменив значение строковой переменной. В код сценария добавлены необязательные строки, повышающие безопасность работы со сценарием. Операционная система не переспросит вас о действительной необходимости удаления пользователя, поэтому в сценарий включен вывод на экран учетных записей, содержащихся в контейнере, для уточнения имени удаляемой учетной записи. Нередко имена состоят всего из трех букв (Ф.И.О.) и могут отличаться лишь одним символом. Вероятность ошибки в этом случае велика, и следует подстраховаться. Приведенный сценарий (листинг 3.14) содержит строки поиска и вывода на экран имен подразделений, что еще не рассматривалось в данной книге. Поэтому фрагменты кода могут быть использованы для создания множества других сценариев, выполняющих различные задачи.

Листинг 3.14. Удаление учетных записей пользователей домена (код del_users.vbs)

```
'*************************************************************************
'del_users.vbs
'вывод пользователей определенной папки или группы,
' подтверждение удаления учетной записи,
' Удаление учетной записи пользователя из домена.
'*************************начало*****************************************
' Определяем область поиска отделов и пользователей
' Можно вручную установить начало поиска
' Примеры: "ou=users,ou=autopark,DC=ap15,DC=dom" - вложенное подразделение
'"cn=users, DC=ap15,DC=dom" - папка users
'"DC=ap15,DC=dom" - весь домен
ContainerPuth = "ou=users,ou=autopark,DC=ap15,DC=dom"
Set Container = GetObject("LDAP:// " & ContainerPuth)
i=0
'Выбираем отдел
For Each organizationalUnit In Container
  i=i+1
  OName = organizationalUnit.Name
    Str = Str & VbCrLf & i & " " & organizationalUnit.Name
      If MsgBox (str,vbYesNo,"Выбираем отдел")=vbYes Then
      ' запоминаем имя отдела
            OnameYes = Oname & "," & ContainerPuth
            Exit For
      End If
Next
' ищем пользователя
Set Object = GetObject("LDAP:// " & OnameYes)
Object.Filter = Array ("User")
i=0
For Each User In Object
      i=i+1
      StrTxt = StrTxt & VbCrLf & i & " " & User.samAccountName & " " &
User.name
Next
MsgBox strtxt
StrTxt = ""
UN=InputBox ("Введите accaunt пользователя","Удаление уч.зап.
пользователя","x")
' Ищем учетную запись и выводим дополнительные сведения о ней
For Each User In Object
      StrTxt = StrTxt & VbCrLf & User.samAccountName & " " & User.name
```

```
        If User.samAccountName = UN Then
       ' Если не было ни одного входа в сеть  LastLogin = 01.01.1930 00:00:00
              Messg = User.LastLogin
              If Err.Description <> "" Then Messg = "01.01.1930 00:00:00"
         Err.Clear
         ' Если согласны, — удаляем учетную запись
                     If MsgBox ("Удаляется: " & User.samAccountName & " "
& User.name _
 & " " & Messg,vbYesNo,"ПРЕДУПРЕЖДЕНИЕ!") = vbYes Then
' !!!!со следующей строки снимите комментарий после отладки скрипта!!!!!
                     'Object.Delete "User",  User.name
                     MsgBox "Учетная запись " & User.name & " удалена!"
                     End If
        End If
Next
StrTxt = ""
i=0
For Each User In Object
        i=i+1
        'StrTxt = StrTxt & VbCrLf & User.AdsPath & VbCrLf
        StrTxt = StrTxt & VbCrLf & i & " " & User.samAccountName & " " &
User.name
Next
set FSO = CreateObject("Scripting.FileSystemObject")
txtlog = "Us.txt"
' Записываем список оставшихся пользователей подразделения в файл
set LogFile = FSO.CreateTextFile(txtlog, True)
        LogFile.WriteLine  Date & " " & Time &  VbCrLf & strtxt
LogFile.Close

'**************************конец*****************************************
```

В коде сценария оставлены реальные имена объектов, по которым легче ориентироваться, чтобы заменить их на свои.

Изменение пароля пользователя

Изменение пароля может быть выполнено самим пользователем, если в свойствах учетной записи установлены соответствующие свойства. Но иногда у администратора возникает необходимость изменить пароль пользователя (листинг 3.15). Например, есть несколько учетных записей, применяемых для временных пользователей, пароли которых известны администратору. После завершения работы временного пользователя необходимо сменить пароль учетной записи.

Листинг 3.15. Код сценария ChangePassword.vbs для изменения пароля пользователя

```
'*************************************************************************
' ChangePassword.vbs
' Изменение свойств учетной записи пользователя.
' Необходимо ввести старый и новый пароли.
'************************начало*****************************************
' Определяем область поиска подразделений и пользователей
' Можно вручную установить начало поиска
' Примеры: "ou=users,ou=autopark,DC=ap15,DC=dom" - вложенное подразделение
'"cn=users, DC=ap15,DC=dom" - папка users
'"DC=ap15,DC=dom" - весь домен
ContainerPuth = "ou=users,ou=autopark,DC=ap15,DC=dom"
Set Container = GetObject("LDAP:// " & ContainerPuth)

i=0
' Выбираем отдел
For Each organizationalUnit In Container
  i=i+1
  OName = organizationalUnit.Name
    Str = Str & VbCrLf & i & " " & organizationalUnit.Name
       If MsgBox (str,vbYesNo,"Выбираем отдел")=vbYes Then
       ' запоминаем имя отдела
             OnameYes = Oname & "," & ContainerPuth
             Exit For
       End If
Next
' ищем пользователя
Set Object = GetObject("LDAP:// " & OnameYes)
Object.Filter = Array ("User")
i=0
For Each User In Object
       i=i+1
       StrTxt = StrTxt & VbCrLf & i & " " & User.samAccountName & " " &
User.name
Next
MsgBox strtxt
StrTxt = ""
UN=InputBox ("Введите accaunt пользователя","Изменение уч. зап.","x")
' Ищем учетную запись и выводим дополнительные сведения о ней
For Each User In Object
       StrTxt = StrTxt & VbCrLf & User.samAccountName & " " & User.name
```

```
      If User.samAccountName = UN Then
      ' Если не было ни одного входа в сеть  LastLogin = 01.01.1930 00:00:00
            Messg = User.LastLogin
            If Err.Description <> "" Then Messg = "01.01.1930 00:00:00"
       Err.Clear
       ' Если согласны, - удаляем учетную запись
If MsgBox ("Изменяем: " & User.samAccountName & " " & User.name & " " & _
Messg,vbYesNo,"ПРЕДУПРЕЖДЕНИЕ!")=vbYes Then
OldPassword = InputBox ("Введите старый пароль...", _
"Изменение пароля","123456")
NewPassword = InputBox ("Введите новый пароль...", _
"Изменение пароля","123456")
' !!!!со следующей строки снимите комментарий после отладки скрипта!!!!!
                        'User. OldPassword, NewPassword
                        MsgBox "Пароль " & User.name & " изменен!"
                  End If
      End If
Next
'**********************конец*****************************************
```

Изменение прав пользователя

Права пользователя могут быть установлены непосредственно для его учетной записи, но обычно все разрешения назначаются группе, а пользователя только включают в эту группу. Такой метод позволяет более гибко управлять правами, а также оперативно добавлять необходимые права. Для контроля наличия каких-либо прав пользователя достаточно получить список групп, в которые он входит. Следующий сценарий (листинг 3.16) позволяет добавить в группу пользователя и тут же посмотреть перечень групп, в которых он состоит.

Листинг 3.16. Код UsersToGroups.vbs для добавления пользователя в группу

```
'**********Добавление пользователя в группу*************
'RootPath - введите корневую область размещения группы и пользователей
'Перечисление групп, в которые входит пользователь.
'Требуются права администратора домена или сервера.
'**********Начало************************************************
ADS_PROPERTY_APPEND = 3
On Error Resume Next
RootPath = ",ou=autopark,dc=ap15,dc=dom"
PathUsers = ",ou=Upravlenie,ou=Users"
PathGroup = ",ou=Groups"
```

```
GroupName=InputBox("Введите имя группы","Управление правами","Group")
UserName=InputBox("Введите имя пользователя","Управление правами","User")

Set Group = GetObject("LDAP:// cn=" & GroupName & PathGroup & RootPath)
Group.PutEx ADS_PROPERTY_APPEND,"member",Array("cn=" & UserName &
PathUsers & RootPath)
Group.SetInfo
If Err.Number=0 Then
MsgBox "Пользователь " & UserName & " добавлен в группу " & GroupName
Else
MsgBox "Ошибка " & Err.Description & " ! " & "Пользователь " & UserName &
"НЕ добавлен в группу " & GroupName
Err.Clear
End If

'*****Проверяем, в каких группах состоит пользователь*************

Const E_ADS_PROPERTY_NOT_FOUND  = &h8000500D

Set objUs = GetObject("LDAP:// cn=" & UserName & PathUsers & RootPath)
    WScript.Echo objUs.Name & " Член групп: "
      arrMemberOf = objUs.GetEx("memberOf")
    If Err.Number <>  E_ADS_PROPERTY_NOT_FOUND Then
        For Each Group in arrMemberOf
        WScript.Echo vbTab & Group
        Next
    Else
        WScript.Echo vbTab & "Групп не найдено"
        Err.Clear
    End If
'**********************Конец************************************
```

Информация о группах, к которым принадлежит пользователь, выводится только на экран. Сценарий можно применить и просто для просмотра списка групп без добавления пользователя в группу. Для этого достаточно в окне ввода информации о группе ввести неверные данные или не вводить ничего. После сообщения об ошибке добавления пользователя к группе будет показан список групп, в которые он входит. Для изменения путей к месту размещения группы и пользователя скорректируйте переменные `RootPath`, `PathUsers`, `PathGroup` в начале сценария.

Примечание

При вводе имени пользователя следует вводить именно имя учетной записи, а не имя входа в сеть.

Изменение параметров учетной записи пользователя

Множество параметров учетной записи пользователя подлежит изменению с помощью сценариев. Это может быть фамилия вышедшей замуж сотрудницы, номер телефона, номер офиса, описание и т. д. В приведенном сценарии (листинг 3.17) есть возможность изменить десять параметров. При желании их список может быть увеличен.

Листинг 3.17. Изменение параметров учетной записи

```
'**********Изменение параметров учетной записи******************
'RootPath – введите корневую область размещения пользователей
'PathUsers – введите путь к пользователю
'Требуются права администратора домена.
'*********Начало************************************************
On Error Resume Next
'Все пользователи находятся в OU autopark
RootPath = ",ou=autopark,dc=ap15,dc=dom"
'Данный пользователь в ou Upravlenie, вложенном в ou Users
PathUsers = ",ou=Upravlenie,ou=Users"
UserName = InputBox _
("Введите имя учетной записи","Меняем параметры учетной записи","xxx")
Const ADS_PROPERTY_UPDATE = 2
Set objUser = GetObject("LDAP:// cn=" & UserName & PathUsers & RootPath)
objUser.Put "givenName", InputBox _
("Введите новое имя","Старое имя: " &
objUser.givenName,objUser.givenName)
objUser.Put "initials", InputBox _
("Введите новые инициалы","Старые инициалы: " &
objUser.initials,objUser.initials)
objUser.Put "sn", InputBox _
("Введите фамилию","Старая фамилия: " & objUser.sn,objUser.sn)
objUser.Put "displayName", InputBox _
("Новое выводимое имя","Старое  выводимое имя: " &
objUser.displayName,objUser.displayName)
objUser.Put "physicalDeliveryOfficeName", InputBox _
("Новый офис","Старый офис: " & _
 objUser.physicalDeliveryOfficeName,objUser.physicalDeliveryOfficeName)
objUser.Put "telephoneNumber", InputBox _
("Введите телефон","Старый телефон: " &
objUser.telephoneNumber,objUser.telephoneNumber)
objUser.Put "mail", InputBox _
("Введите E-mail","Старый E-mail: " & objUser.mail,objUser.mail)
```

```
objUser.Put "wWWHomePage", InputBox _
("Введите домашнюю страницу","Старая страница: " &
objUser.wWWHomePage,objUser.wWWHomePage)

objUser.PutEx ADS_PROPERTY_UPDATE, "description", Array(InputBox _
("Введите описание","Описание: ",objUser.description))
objUser.PutEx ADS_PROPERTY_UPDATE, "url", Array(InputBox _
("Введите URL","URL: ",objUser.url))
MsgBox Err.Description
objUser.SetInfo
 '**********Конец**************************************************
```

Данный сценарий довольно хорошо защищен от ошибок администратора. По умолчанию, когда изменения не вносятся, но нажимается кнопка **OK**, все параметры остаются без изменений. Если имя учетной записи не существует в домене, сценарий прекратит работу с сообщением об ошибке.

Создание группы

Необходимость создания списков, связанных с выполнением единой задачи разрешений, применяемых для группы пользователей, определяет потребность в создании группы, в которую должны входить эти пользователи. Создание новой группы — процедура несложная, и возможность выполнить эту процедуру с обычной рабочей станции вашей сети достаточно заманчива. В самых различных областях промышленности идет процесс автоматизации производства. Есть цеха, работающие под наблюдением одного оператора. Ваша сеть — это тоже цех, и намного приятнее быть оператором в автоматизированном производстве, чем героем-многостаночником, снующим от станка к станку. Чем реже возникает необходимость подходить к серверу или другим рабочим станциям, тем лучше организована ваша работа. Для сети, включенной в Active Directory, наибольшее значение имеют глобальные группы, которые можно включать в локальные группы рабочих станций, предоставляя права для подключения к ним сетевым пользователям.

Следующий сценарий (листинг 3.18) содержит процедуру создания глобальной группы, входящей в подразделение (организационную единицу).

Листинг 3.18. Создание глобальной группы

```
'**********Создание новой группы**************
'ИМя - NewGroup.vbs

'Требуются права администратора домена
'**********Начало**************************************************
```

```
Set objOU = GetObject("LDAP:// ou=groups, OU=autopark,dc=ap15,dc=dom")
Set objGroup = objOU.Create("Group", "cn=NewTestGroup")
objGroup.Put "sAMAccountName", "NewTestGroup"
objGroup.SetInfo
'*********Конец*****************************************************
```

Если группа была создана ошибочно или просто требуется ее удаление, можно воспользоваться следующим сценарием (листинг 3.19).

Листинг 3.19. Удаление группы

```
'**********Удаление группы*************
'Имя -- DelGroup.vbs

'Требуются права администратора домена
'*********Начало*****************************************************

Set objOU = GetObject("LDAP:// ou=groups, OU=autopark,dc=ap15,dc=dom")
Set objGroup = objOU.Delete("Group", "cn=NewTestGroup")
'*********Конец******************************************************
```

Общий доступ файлам и папкам

Создав группу, в которую вы уже можете поместить пользователей, хорошо бы иметь возможность установить для этой группы права доступа к определенным ресурсам. К сожалению, простого пути для автоматизации этой процедуры нет. Есть возможность предоставить общий доступ к какой-либо папке (листинг 3.20), а затем другими средствами настроить права более тонко.

Листинг 3.20. Назначение общего доступа к папкам

```
'*********Начало*****************************************************
'Общий доступ назначается с присвоением сетевого имени
Const FILE_SHARE = 0
Const MAXIMUM_CONNECTIONS = 9
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate}!\\" & strComputer &
"\root\cimv2")
Set objNewShare = objWMIService.Get("Win32_Share")
errReturn = objNewShare.Create _
    ("C:\SHRf", "NameShare", FILE_SHARE, _
        MAXIMUM_CONNECTIONS, "Описание общего ресурса.")
Wscript.Echo errReturn
'******************Конец*************************************
```

Тем не менее в критической ситуации вам не придется бежать к серверу для ограничения доступа к папке. Следующий сценарий (листинг 3.21) позволяет полностью отменить общий доступ к папке.

Листинг 3.21. Отмена общего доступа к папке

```
'********************Начало*************************************
' Отмена общего доступа
' Отмена общего доступа осуществляется по имени общего ресурса в сети
strComputer = "."

Set objWMIService = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate}!\\" & strComputer &
"\root\cimv2")
Set colShares = objWMIService.ExecQuery _
    ("Select * from Win32_Share Where Name = 'NameShare1'")
For Each objShare in colShares
    objShare.Delete
Next
'*********************Конец**************************************
```

Для изменения максимального числа подключений к ресурсу, его описания и имени в сети можно выполнить последовательно удаление его общего доступа и новое назначение, но с другими параметрами.

Работа сценариев на старых машинах

Работа со сценариями может не только принести пользу, но и предоставить возможность пользователям, не подходя к серверу, управлять им в той степени, которую допускает администратор. Например, общий доступ к ресурсу, который создал пользователь, может быть предоставлен или ограничен самим пользователем. Для выполнения процедуры следует лишь запустить сценарий (необходимо иметь и соответствующие разрешения, установленные заранее администратором). Но до сих пор многие пользователи работают в операционной системе Windows 98. В этой ОС не выполняются сценарии, для работы которых требуются провайдеры WinNT или LDAP (Lightweight Directory Access Protocol, облегченный протокол доступа к каталогам). Провайдер WinNT используется записями SAM (Security Accounts Manager, менеджер защищенного доступа) — либо локальными учетными записями на сервере, либо записями в домене NT 4.0. LDAP используется для учетных записей пользователей в Active Directory. Новые операционные системы поддерживают работу и с провайдером WinNT, и с провайдером LDAP. Но есть

простой способ заставить работать эти сценарии под управлением Windows 98. На дистрибутивном диске Windows 2000 Server, а также по приведенным ниже ссылкам можно получить установочный комплект клиента Active Directory для Windows 9*x* и Windows NT4.0 (Microsoft Active Directory Client Extensions for Windows 9*x* & Windows NT 4.0):

http:// www.mrtech.com/news/messages/1437.html

http:// www.microsoft.com/windows2000/server/evaluation/news/bulletins /adextension.asp

Следует обновить и сервер сценариев Windows Script Host до версии WSH 5.6 с поддержкой русского языка, найдя его по ссылке **http:// msdn.microsoft.com /library**. Проведя такую модернизацию, вы можете применять сценарии для управления Active Directory на старых машинах и компьютерах под управлением Windows 98.

Программы в формате HTA

Этот формат файлов появился относительно недавно, но получает все больше распространение в качестве инструмента для индивидуального применения. Внутри файла могут уживаться сценарии, написанные на различных script-языках. При запуске такой файл выглядит как обычное окно программы. Эти свойства позволяют применить этот формат файлов и в работе администратора.

Для успешной разработки программ в формате HTA (HTML Application) необходимо знание основ создания HTML-страниц и написания сценариев на одном или более script-языке. Для иллюстрации возможностей таких файлов приведем пример программы, выводящей на экран список учетных записей пользователей любого компьютера сети, имя которого будет введено при старте программы (рис. 3.13 и листинг 3.22).

На основе уже рассмотренных или написанных самостоятельно сценариев вы можете создать рабочий комплект программ администратора, удобный в применении, имеющий оконный интерфейс.

Листинг 3.22. Текст HTA-программы

```
<HTML>
<META HTTP-EQUIV="Page-Enter"
CONTENT="revealTrans(Duration=3.0,Transition=14)">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
<font color="yellow" size="2" face="Arial">
  <HEAD>
```

```
  <TITLE>Программы АДМИНИСТРАТОРА</TITLE>
<!--Заголовок страницы'-->
<p align="center"><b>ПОЛЬЗОВАТЕЛИ ДОМЕНА и ДАТА ПОСЛЕДНЕЙ РЕГИСТРАЦИИ
В СЕТИ</b>
<!-- Свойства окна программы -->
<HTA:APPLICATION ID="oHTA" CAPTION="yes" MAXIMIZEBUTTON=NO
MINIMIZEBUTTON=NO>

<!--
После объявления основных свойств страницы скрипт, выводящий список
пользователей в файл users.txt (размещен в заголовке)
**********Начало**********'-->
<SCRIPT LANGUAGE="VBScript">
<!--
DomainName = InputBox ("Введите имя сервера вместо
заполнителей","Пользователи на:","XXXXX")
Set Container = GetObject("WinNT:// " & DomainName)
Container.Filter = Array("User")
 i = 0
        StrTxt = ""
        Messg = ""
        For Each User In Container
            i = i + 1
            On Error Resume Next
            Messg = i
            Messg = Messg & ";" & User.Name
            Err.Clear
            Messg = Messg & ";" & User.FullName
            Err.Clear
            Messg = Messg & ";" & User.LastLogin
            If Err.Description <> "" Then Messg = Messg & ";" &
"01.01.1930 00:00:00"
            Err.Clear
            Messg = Messg & VbCrLf
            StrTxt = StrTxt & Messg
            Err.Clear
        Next

set FSO = CreateObject("Scripting.FileSystemObject")
        txtlog = "Users.txt"
        set LogFile = FSO.CreateTextFile(txtlog, True)
            LogFile.WriteLine  Date & " " & Time &  vbCrLf & strtxt
        LogFile.Close
```

```
'-->
</SCRIPT>
<!--*****************Конец***************'-->

  </HEAD>
<!--Тело страницы'-->
  <BODY BGCOLOR="navy" SCROLL=no onLoad="clock_form()">
<!--Таблица с кнопками'-->
<table border="1" width="100%" bordercolorlight="navy"
bordercolordark="navy" bordercolor="navy" bgcolor="aqua"
cellspacing="1%">
  <tr>
    <td width="15%"><p align="center">
<!--Кнопка с вопросом'-->
<button onclick="clickme()">==?==</button>
      </td>
    <td width="15%">
<!--Кнопка сохранения'-->
<p align="center"><INPUT ID=btnSaveFile TYPE=button VALUE="B
<дата>user.txt" ONCLICK="fileSave()">
</td>
    <td width="15%"> </td>
    <td width="15%"> </td>
    <td width="15%"><p align="center">
<!--Кнопка "ЗАКРЫТЬ!"'-->
<input type="button" value="Закрыть!" onclick="closeIt()">
    </td>
  </tr>
</table>
<!-- Конец таблицы'-->
<!-- Текстовое поле'-->
  <TEXTAREA id=txtArea rows=12 wrap=off cols=36
      style="WIDTH: 735px; HEIGHT: 390px">
  </TEXTAREA>
  <BR>
<!--Скрипт для вывода сообщения кнопки с вопросом'-->
<script language="VBScript">
<!--
   Sub clickme()
     Alert "Для администратора!"
   End Sub
'-->
</script>
<!--Скрипт для вывода сообщения от часов'-->
```

```
<script language="VBScript">
<!--
   Sub mousmove()
     Alert "...И время ни на миг не остановишь!"
   End Sub
'-->
</script>

<!--Скрипт для кнопки сохранения текста в файл'-->
<SCRIPT LANGUAGE="JavaScript"><!--
 var fs = new ActiveXObject("Scripting.FileSystemObject");
  {
    var txtStream = fs.OpenTextFile("Users.txt",1,false);
    txtArea.value = txtStream.ReadAll();
    txtStream.Close();
   }

  function fileSave(){
   temp_date = new Date();
   day = temp_date.getDate();
   month = temp_date.getMonth() + 1;
   year = temp_date.getYear();
  if (day < 10){
    day = "0" + day;
  }
  if (month <10){
    month = "0" + month;
  }
 DT=""
 DT +=day;
 DT +=month;
 DT +=year;
    var txtStream = fs.OpenTextFile(DT+"Users.txt",2,true);
    txtStream.Write(txtArea.value);
    txtStream.Close();
 }
 // '-->
</SCRIPT>

<!--Скрипт для кнопки выхода'-->
<script language="JavaScript"><!--
function closeIt() {
  close();
}
```

```
// -->
</script>
<p align="center">
<!--Часы в подвале страницы'-->
<script language="JavaScript"><!--
function clock_form(){
        day=new Date()
        clock_f=day.getHours()+":"+day.getMinutes()+":"+day.getSeconds()
        document.form.f_clock.value=clock_f
         id=setTimeout("clock_form()",100)
}
// -->
</script>

<form name=form metod="get">
Time is money
<input name=f_clock  maxlength=8 size=3 onmousemove="mousmove()">
</form>
  </BODY>
  </HTML>
```

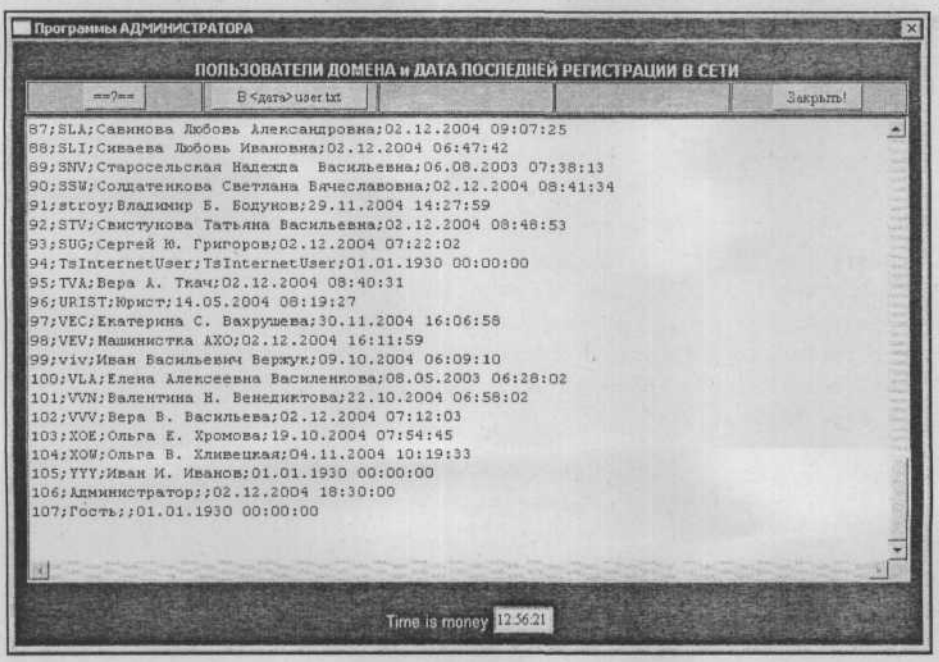

Рис. 3.13. Окно **Программы АДМИНИСТРАТОРА**

Для того чтобы эта программа заработала, достаточно весь ее код поместить в текстовый файл, а затем изменить расширение на hta. В процессе работы программа создает файл users.txt в том же каталоге, где она находится. Содержание текстового окна программы может быть отредактировано. После щелчка на кнопке **B<дата>user.txt** будет создан еще один текстовый файл, в имени которого присутствует дата его создания, а содержание соответствует содержанию текстового окна. При написании собственных HTA-программ следует учесть, что активные сценарии, которые должны выполняться при запуске программы, необходимо помещать в заголовке HTML-кода между тегами <HEAD> и </HEAD>, причем именно в конце заголовка. Кроме того, если вы для редактирования файла используете PrimalScript, пробный запуск программы из этой среды выполнять не стоит. HTA-файлы в этой среде работают некорректно, и запускать их следует отдельно от среды разработки после сохранения изменений. Для уменьшения объема программы в ней не обработана одна ошибка. Если при запуске программы вы откажитесь от сбора сведений о пользователях, на экран будет выведено сообщение об ошибке, после чего будет показан список учетных записей, полученный при последнем нормальном запуске программы.

Возможно, вам не сразу удастся запустить все инструменты, описанные в данной главе. Внимательно проверьте код сценариев и программ HTA. Все без исключения примеры действительно работают в реальной сети автора.

ГЛАВА 4

Управление политикой доступа к информации

Организовать сеть с необходимыми сервисами, создать группы пользователей и их учетные записи, обеспечив их необходимыми правами, дающими возможность использовать эти сервисы, — это еще не все, что необходимо для нормальной работы сети. Значительная доля труда администратора сети должна быть направлена на управление политикой доступа к информации. Всегда есть папки и файлы, к которым необходим доступ многих людей, и наоборот, такие, к которым может иметь доступ очень ограниченный круг пользователей. Правильно организованный доступ к устройствам печати позволяет легче ориентироваться при выборе необходимого сетевого принтера. Иногда структура предприятия очень "неудобна" для администратора сети. Возникают противоречивые требования, связанные с запрещением доступа к файлам и разрешением доступа к принтерам, находящимся в одном отделе. Схемы организации доступа к различным объектам сети предприятия могут быть очень разнообразны, но общие принципы должны быть всегда одни. Часто запрет на доступ к отдельным объектам сети носит достаточно условный характер, но позволяет правильно организовать работу сети. В данной главе будут рассмотрены примеры реализации различных требований к политике доступа к информации.

Группы уровня доступа

Доступ к информации в сети может контролироваться различными путями, начиная от ограничений на уровне файловой системы и заканчивая ограничениями на уровне применяемых приложений. Причем последнее ограничение часто довольно условно. Если, например, пользователь получает информацию из сетевого приложения, написанного в среде MS Access, то ограничения на уровне программы не позволят ему запустить процессы, которые

ему не требуются в служебных целях (обычно в таких приложениях доступ к необходимым функциям определяется паролем). В то же время сама база данных, к которой обращается клиентское приложение, может быть не защищена. В этом случае продвинутый пользователь имеет возможность получить из этой базы данных любую интересующую его информацию. Более того, он способен изменить структуру базы данных, нарушив целостность самих данных и корректность работы приложений. Для обеспечения правильной организации доступа к данным следует внимательно изучить все возможные пути обхода установленных ограничений и перекрыть эти пути. Конечно, в небольшом коллективе, в котором каждый сотрудник на виду и все заинтересованы в успешной работе коллектива, вряд ли найдется злоумышленник. Тем не менее возможны просто ошибки. Если вы имели опыт работы с базами данных, то можете себе представить, что удалить данные — задача довольно легкая, куда сложнее их восстановить. А ведь именно удаление данных возможно не по злому умыслу, когда полный доступ к ним открыт пользователям, не несущим ответственности за их сохранность.

Определить и установить права для каждого пользователя сети, — такая задача может быть слишком трудоемкой. Поэтому во всех вариантах доступа к данным применяются группы. Мы не будем глубоко анализировать теорию организации групп в сетях, но отметим, что группы доступа существуют, начиная с рабочих станций и заканчивая самыми верхними структурами сети. В нашем случае такой верхней структурой может быть домен. Группы могут содержать как отдельных пользователей, так и другие группы. Подключая рабочую станцию с ОС Windows XP к домену, мы автоматически включаем группу администраторов домена в группу администраторов компьютера. Права, определенные групповыми политиками и файловой системой, назначенные группе, будут применены и ко всем членам этой группы. В современных операционных системах Windows существуют встроенные готовые шаблоны безопасности, представляющие собой отправную точку в создании политик безопасности, которые настраиваются, чтобы удовлетворять организационным требованиям. Шаблоны можно настраивать при помощи оснастки **Шаблоны безопасности**. После настройки готовых шаблонов безопасности их можно использовать для изменения конфигурации компьютеров сети. Изменить конфигурацию безопасности компьютеров можно при помощи оснастки **Анализ и настройка безопасности**, утилиты Secedit.exe, работающей из командной строки, а также при помощи импорта шаблона в оснастку **Локальная политика безопасности**. Можно изменять конфигурацию нескольких компьютеров, импортировав шаблон в компонент **Параметры безопасности**, являющийся расширением оснастки **Групповая политика**. На основе шаблонов безопасности можно также выполнять анализ возможных слабых мест безопасности и нарушений политики системы при помощи оснастки

Анализ и настройка безопасности. Мы же пока обратимся только к оснастке **Локальные параметры безопасности** (рис. 4.1), имеющейся на любом компьютере с операционной системой, начиная с Windows 2000, и оснасткам **Политика безопасности домена** и **Политика безопасности контроллера домена**, которые есть на сервере вашей сети.

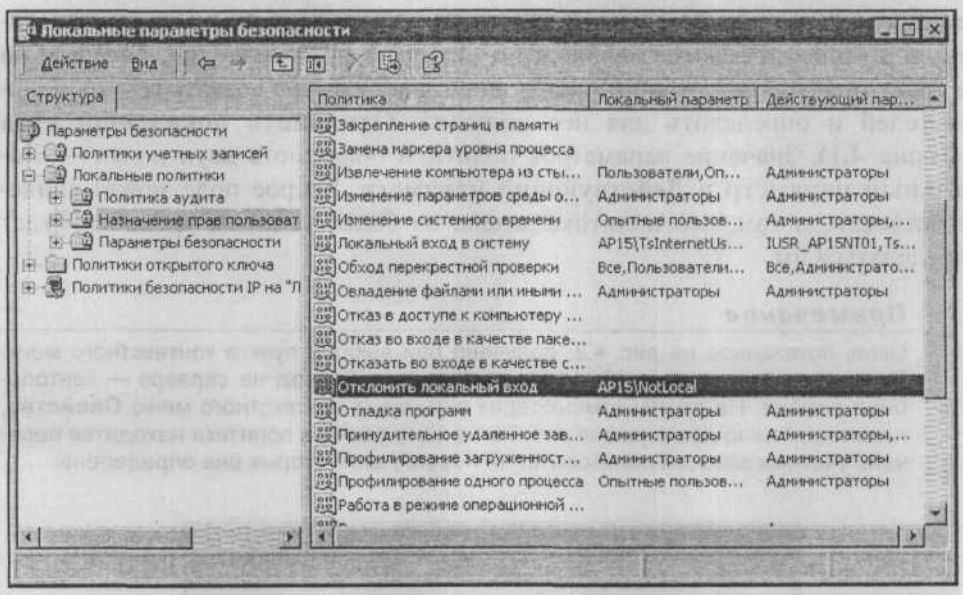

Рис. 4.1. Оснастка **Локальные параметры безопасности** (политика **Отклонить локальный вход в систему**)

Как следует из названий оснасток, они позволяют управлять политикой безопасности на различных уровнях. Это уровни локальный, контроллера домена и домена в целом. Если аналогичные политики есть на всех уровнях, то действовать будет политика, определенная на самом верхнем из них. По умолчанию большая часть политик вообще не определена, что позволяет начинать настройки с любого уровня. Наибольшее число политик по умолчанию определено на локальном уровне, они определяют безопасность именно компьютера, на котором установлен сервер. Определяя политики безопасности домена, можно установить параметры безопасности и права пользователей домена. Собственно говоря, количество политик, имеющихся в этих оснастках, таково, что с первого раза (и даже с десятого) вы не запомните назначение каждой из них. Но в большинстве случаев это и не требуется. Важно понимать, какого результата вы хотите добиться, и выбирать соответствующее средство для его достижения.

Ограничение прав локального входа в систему на сервере

Если мы имеем несколько уровней безопасности, то это не значит, что они определяются совершенно независимо. Очевидно, что, получив доступ к локальной системе сервера, можно нарушить работу целого домена намеренно деструктивными или неумелыми действиями. Отсюда вывод — доступ к серверу в локальном режиме необходимо запретить пользователям, которым он не требуется. Для реализации такого запрета достаточно создать группу пользователей и определить для нее политику **Отклонить локальный вход** (см. рис. 4.1). Значение параметров политики показано в двух полях — **Локальный параметр** и **Действующий параметр**. Второе поле может свидетельствовать о том, что политика задана на более высоком уровне и будет определяться им.

Примечание

Окно, показанное на рис. 4.2, получено при выборе пункта контекстного меню **Безопасность** политики **Отклонить локальный вход** на сервере — контроллере домена. На других компьютерах есть пункт контекстного меню **Свойства**, и выглядит окно несколько иначе. Там в окне свойств политики находится перечень учетных записей пользователей и групп, для которых она определена.

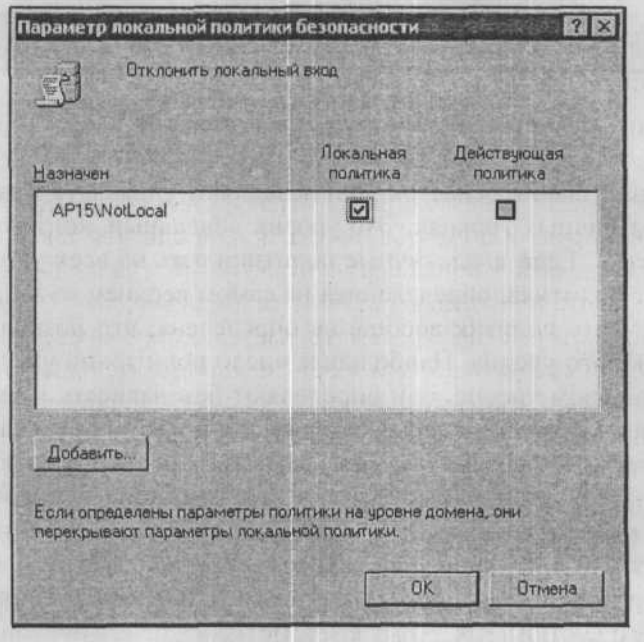

Рис. 4.2. Настройка параметра безопасности

Любая учетная запись пользователя или группа, помещенная в эту группу, потеряет возможность локального входа на сервер, но вход по сети будет разрешен, если он был разрешен ранее для этих пользователей и групп.

Группы, создаваемые в домене, должны определять вполне конкретные права пользователей, входящих в них, и права эти не должны противоречить друг другу. В этом случае есть возможность определить структуру групп в соответствии с требованиями вашей организации. Часть групп создана по умолчанию и может быть применена к отдельным пользователям. Наивысшими правами как на компьютере, так и в домене пользуется учетная запись администратора домена, далее следуют участники группы администраторов домена, завершают список группа гостей и встроенная учетная запись гостя. Встроенные учетные записи и группы удалять не стоит. При необходимости вы можете просто отключить отдельные учетные записи. Создавая новые группы, их можно помещать друг в друга и в группы, созданные по умолчанию. Существуют и могут быть созданы как локальные группы компьютера (сервера), так и локальные и глобальные группы домена. Обычно на уровне домена применяют глобальные доменные группы. Для каждой группы определяется свой набор политик и уровней доступа к ресурсам, к которым предполагается доступ пользователей, входящих в эти группы. В результате создается иерархия групп, отличающихся своими правами, а пользователи — члены этих групп получают права в диапазоне от полного доступа ко всем ресурсам и во всех режимах до полного отсутствия доступа к чему бы то ни было. Обычно такими крайними точками являются учетная запись администратора домена и гостя.

Следует отметить тот факт, что на компьютере — контроллере домена не существуют локальные учетные записи пользователей (рис. 4.3).

Следовательно, каждая действующая учетная запись на контроллере домена имеет некоторые права в домене. Отсюда можно сделать такой вывод: если вы решили организовать Web-сервис или почтовый сервис, доступный извне, то это следует делать на отдельном компьютере, поскольку "Береженого Бог бережет". В сети, которая здесь рассматривается, таким компьютером является второй сервер, исполняющий эти и другие вспомогательные роли. Средства, имеющиеся в распоряжении хакеров и прочих "доброжелателей", могут быть достаточно совершенными, чтобы прослушать вашу сеть и перехватить пароли, или проникнуть в нее другим путем. Отдельно стоящий компьютер, не имеющий никаких прав в домене, будет дополнительным препятствием для проникновения в вашу сеть. В то же время пользователи Web- и почтового сервиса не должны иметь прав на вход в систему не только локально, но и по локальной сети. Конечно, вариантов организации структуры сети множество, мы же рассмотрим примеры, которые помогут сориентироваться при определении варианта настройки своей сети.

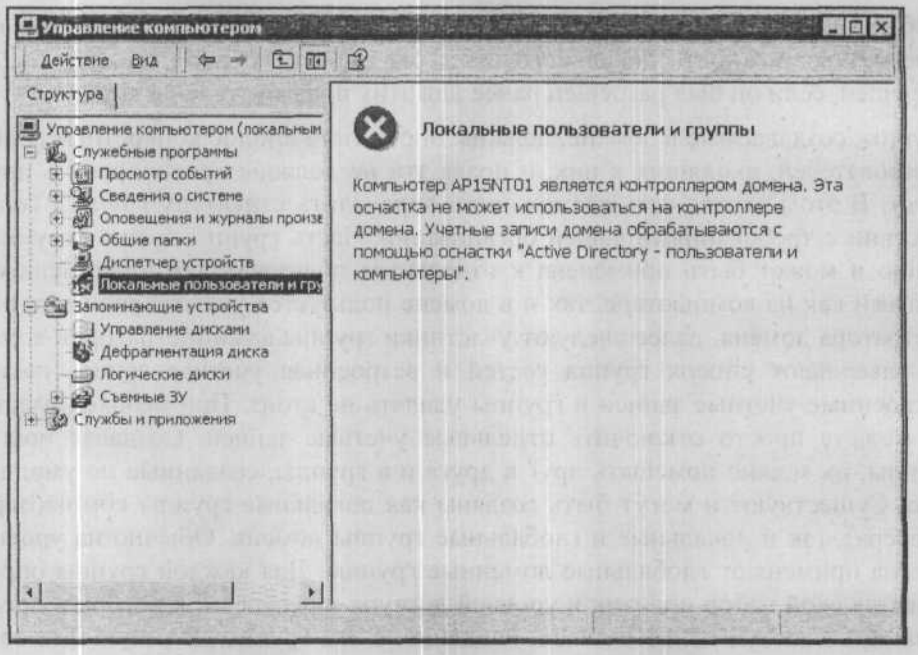

Рис. 4.3. Отсутствие локальных учетных записей на контроллере домена

Права помощника администратора

Выполняя работы по администрированию своей сети, вы будете вынуждены иногда часть задач возлагать на другого человека. Возможно, вы уходите в отпуск или просто объем работы достаточно велик. Но доверять полный ничем не ограниченный доступ к серверу и к сети можно только себе (и то не всегда). Поэтому при организации учетной записи для вашего помощника следует определить тот необходимый минимум прав, который позволит ему выполнять свои обязанности, но в значительной степени исключит вероятность возникновения проблем, связанных с превышением имеющихся полномочий (возможно, и невольным).

Определите круг задач вашего помощника. Предположим, что в ваше отсутствие потребуется добавлять и удалять учетные записи пользователей. Причем вам не хотелось бы допускать выполняющего это человека непосредственно к серверу.

Для решения таких задач достаточно в служебных целях создать учетную запись, владелец которой не будет иметь права на локальный вход на сервер. При этом выполнение сетевого входа возможно, но и его необходимость условна. В *главе 3* были рассмотрены сценарии для управления учетными запи-

сями. Средой для выполнения этих сценариев является оболочка, создаваемая программой Wscript.exe. Под управлением Windows XP можно запускать сценарии от имени другого пользователя, не выходя из своего сеанса. Для этого достаточно написать командный файл, содержащий строку:

```
runas /user:ap15.dom \<имя_учетной_записи> "wscript.exe
c:\scripts\<имя_файла>.vbs"
```

где `c:\scripts\script.vbs` — путь и имя файла сценария, который будет выполняться, а `runas` — это команда, позволяющая запустить программу от имени другой учетной записи. В ОС Windows XP и Windows Server 2003 эта команда добавлена и в контекстные меню ярлыков программ в виде пункта **Запуск от имени...**.

Примечание

В тексте сценария должен быть указан полный путь к создаваемым текстовым файлам, чтобы не возникли трудности с их поиском в том случае, если они созданы от имени разных пользователей.

Вашему помощнику потребуется лишь знание пароля учетной записи, которую вы для него создали. Этот пароль необходимо ввести после запуска командного файла (рис. 4.4).

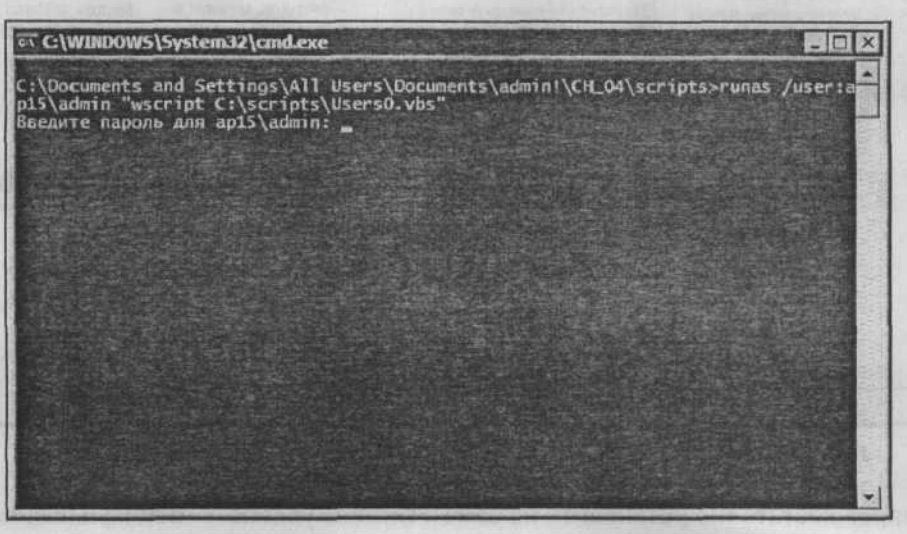

Рис. 4.4. Запуск сценария из командного файла от имени администратора

Лучше, если ограничение на право локального входа в систему на сервере будет установлено для отдельной группы, например, **NotLocal**. В эту группу следует включить и учетную запись помощника администратора. Для того чтобы этот пользователь мог управлять другими учетными записями, он дол-

жен быть членом группы операторов учета (встроенная группа). В свою очередь, группе операторов учета не должно быть предоставлено право локального входа в систему.

Ограничение локального входа в систему может быть установлено локальными политиками в контейнере дерева консоли **Локальные параметры безопасности | Назначение прав пользователя | Локальный вход в систему/Отклонить локальный вход**. Политики эти имеют три уровня:

- Локальные политики безопасности
- Политики безопасности домена
- Политики безопасности контроллера домена

Политики более высокого уровня перекрывают действие нижестоящих политик. Таким образом, группе **Операторы учета** не должны быть установлены разрешения на локальный вход (рис. 4.5), а группе **NotLocal** необходимо установить запрет на локальный вход (политика **Отклонить локальный вход**).

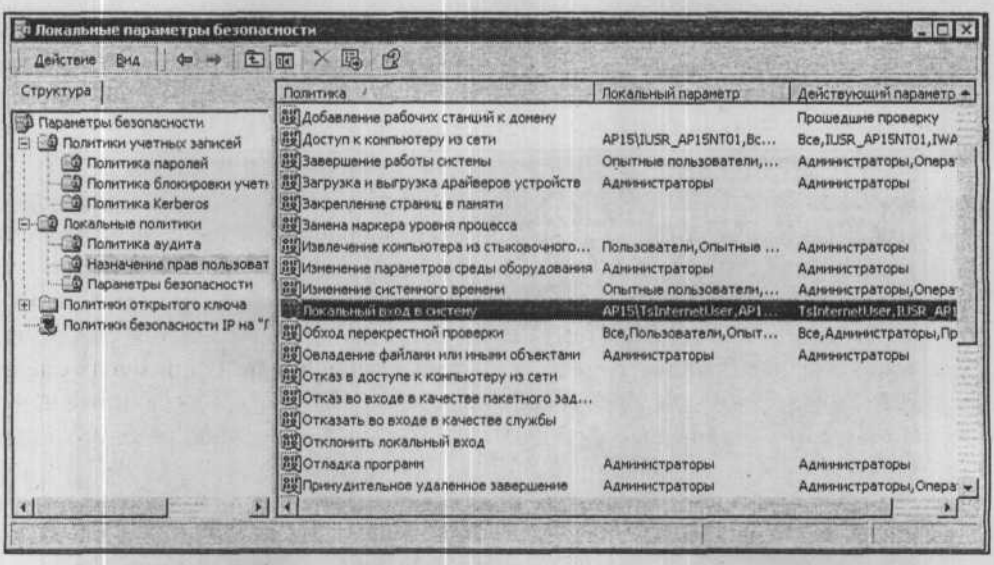

Рис. 4.5. Окно **Локальные параметры безопасности (Локальный вход в систему)**

Запрет достаточно установить на самом низком уровне — в локальных политиках. В табл. 4.1 показан возможный вариант распределения записей о группах в политиках безопасности. Запись "Не определена" говорит о том, что эта политика не применяется на данном сервере, но если она применяется на вашем сервере, то должно стоять слово "Отсутствует", группа не должна входить в перечень этой политики.

Таблица 4.1. *Распределение групп в политиках безопасности*

Уровень политики	Политика	Группа *NotLocal*	Группа *Операторы учета*
Локальные	Локальный вход в систему	Отсутствует	Отсутствует
	Отклонить локальный вход	Присутствует	Отсутствует
Домена	Локальный вход в систему	Не определена	Не определена
	Отклонить локальный вход	Не определена	Не определена
Контроллера домена	Локальный вход в систему	Отсутствует	Отсутствует
	Отклонить локальный вход	Не определена	Не определена

Если ваш помощник должен выполнять задачи по администрированию только второго сервера, не являющегося контроллером домена, то для него можно создать еще несколько сценариев, используя заготовки, приведенные ниже.

При необходимости создания учетной записи пользователя на втором сервере, чтобы поручить кому-либо выполнение операций по настройке сервера, она может быть создана временно, а затем удалена. Аналогично, можно создавать и удалять группы, от пользователей можно требовать изменить пароль при следующем входе в систему. Все эти действия допускается совершать удаленно с вашего рабочего места с помощью сценариев. В примерах сценариев, которые уже были рассмотрены, приводилось много дополнительных функций, таких, например, как сохранение информации в файле, интерактивный режим работы со сценарием. В следующих примерах (листинги 4.1—4.6) этих дополнительных функций нет, приведены только фрагменты, хотя и полнофункциональные. Но вы можете позаимствовать недостающие функции из сценариев, которые были приведены в *главе 3*. Если нет желания изменять текст сценария, то, заменив имя компьютера, пользователя и группы на необходимые, поместите приведенные фрагменты в текстовые файлы и измените их расширение на vbs. Получатся рабочие скрипты.

Листинг 4.1. Добавление новой учетной записи пользователя

```
strComputer = "Server2"
Set colAccounts = GetObject("WinNT://" & strComputer & "")
```

```
Set objUser = colAccounts.Create("user", "TestUser")
objUser.SetPassword "test"
objUser.SetInfo
```

Листинг 4.2. Удаление учетной записи пользователя

```
strComputer = "Server2"
strUser = "TestUser"
Set colAccounts = GetObject("WinNT://" & strComputer & "")
objComputer.Delete "user", strUser
Пример 21-3/(42)
'Создание новой группы
strComputer = "Server2"
Set colAccounts = GetObject("WinNT://" & strComputer & "")
Set objUser = colAccounts.Create("group", "Новая группа")
objUser.SetInfo
```

Листинг 4.3. Добавление пользователя в группу

```
strComputer = "Server2"
Set objGroup = GetObject("WinNT://" & strComputer & "/Новая
группа,group")
Set objUser = GetObject("WinNT://" & strComputer & "/TestUser,user")
objGroup.Add(objUser.ADsPath)
```

Листинг 4.4. Добавление группы в группу

```
strComputer = "Server2"
Set objGroup = GetObject("WinNT://" & strComputer &
"/Пользователи,group")
Set objUser = GetObject("WinNT://" & strComputer & "/Новая группа,group")
objGroup.Add(objUser.ADsPath)
```

С помощью этого сценария можно включать новую группу в любую уже существующую. При этом пользователи, входящие в новую группу, получают соответствующие права.

Листинг 4.5. Удаление группы

```
strComputer = "Server2"
Set objComputer = GetObject("WinNT://" & strComputer & "")
objComputer.Delete "group", "Новая группа"
```

```
Пример 21-7/(46)
'Список групп с вложенными группами и пользователями
strComputer = "Server2"
Set colGroups = GetObject("WinNT://" & strComputer & "")
colGroups.Filter = Array("group")
For Each objGroup In colGroups
    Wscript.Echo objGroup.Name
    For Each objUser in objGroup.Members
        Wscript.Echo vbTab & objUser.Name
    Next
Next
```

Листинг 4.6. Требование изменить пароль при следующем входе в систему

```
strComputer = "Server2"
Set objUser = GetObject("WinNT:// " & strComputer & "/TestUser ")
objUser.Put "PasswordExpired", 1
objUser.SetInfo
```

Итак, помощник администратора, не имея прав на локальный вход в систему на сервере, при помощи сценариев сможет управлять учетными записями пользователей: создавать их, изменять, удалять, а также просматривать списки и свойства записей.

Внимательно изучив возможности, предоставляемые политиками безопасности, можно очень гибко настроить права различных групп и отдельных пользователей.

Внимание!

Проводя настройки политик безопасности, внимательно следите за тем, чтобы не лишить своих прав администраторов домена и компьютера. Это может привести к полной неуправляемости домена.

Диапазон прав и запретов, которые могут быть назначены пользователям, очень широк. Администраторы (есть несколько встроенных учетных записей с разными правами) обладают практически неограниченными возможностями, гости — наоборот, имеют очень мало прав. Но есть пользователи, которые по умолчанию имеют очень специфические права, специальная настройка которых не требуется. К таким особенным учетным записям могут относиться пользователи почтового сервера.

Бесправные пользователи почты

Настраивая почтовый сервер *(см. главу 2)*, мы выбрали для учетных записей пользователей почты вариант авторизации по локальным учетным записям

Windows. При этом для каждого почтового ящика при его создании учетные записи с соответствующими правами формируются автоматически. Права этих пользователей настолько ограничены, что они не могут войти в систему ни локально, ни по сети. Посмотрев в оснастке **Управление компьютером** на втором сервере свойства этих пользователей, вы увидите, что они являются членами одной-единственной группы **POP3User**. В свойствах локальной политики безопасности **Отклонить локальный вход** вы увидите эту группу. Политика **Отказ в доступе к компьютеру из сети** для этой группы не определена, поскольку членам группы необходимо получать доступ к своим почтовым ящикам, в то же время явно для этой группы не указаны разрешения на доступ к папкам — почтовым ящикам, поскольку этот доступ осуществляется только посредством почтового сервера. Все пользователи этого сервера включены еще в несколько специальных групп, имена которых отсутствуют в перечне групп, содержащемся в папке **Группы**. Это встроенные группы, определяющие специфические права тех пользователей, кому не даны явные права на доступ к файлам и папкам. Изменять права для автоматически созданных пользователей не требуется, если только вы не хотите их расширить. Если же такая необходимость возникла, то не изменяйте права конкретного пользователя, а поместите его в существующую или вновь созданную группу, для которой и определите соответствующие права.

"Изолированные" подсети

Случается, что требования к защите информации создают трудно разрешимые ситуации. Так например, в одной организации перед администратором была поставлена следующая задача: группа пользователей (руководители) должна получать некоторую информацию в виде распечаток на принтере от другой группы (подчиненные), а также иметь возможность доступа к информации на компьютерах подчиненной группы. При этом подчиненная группа не должна иметь доступ к информации в группе руководителей, а также видеть компьютеры этой группы в сетевом окружении.

Как наиболее надежный вариант решения такой задачи, можно предложить организацию двух доменных сетей, соединенных маршрутизатором. Для организации печати при этом можно применять принт-серверы, доступные для всех пользователей... Но задачу необходимо было решить без приобретения дополнительного оборудования.

При кажущейся на первый взгляд относительной простоте задачи решить ее, не выходя за рамки обычной структуры локальной сети, вы, вероятнее всего, не сможете. Но с определенным допуском на уровень защиты информации, а также на некоторые неудобства при пользовании отдельными сетевыми сервисами, проблема может быть решена без дополнительных затрат, если...

компьютеры группы руководителей исключить из домена. При этом сами коммуникации и физическая структура сети не изменятся, а логически сеть преобразуется в две.

Компьютеры, выведенные из домена, должны войти в состав рабочей группы, имя которой *не должно* совпадать с именем домена. IP-адреса этих компьютеров могут соответствовать адресам из диапазона зарезервированных адресов *(см. главу 1)*.

Для обеспечения доступа к принтерам, подключенным к рабочим станциям группы руководителей, необходимо выполнить несколько изменений в настройках этих рабочих станций. Откройте **Локальная Политика Безопасности | Локальные политики | Параметры безопасности**.

На рис. 4.6 приведены два варианта соответствующего окна настроек, изображение которого получено на разных рабочих станциях, а вид зависит от индивидуальных предпочтений пользователя и варианта локализации ОС. В этом окне следует найти три параметра, перечисленные ниже.

- **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей (Network access: Sharing and security model for local accounts).**

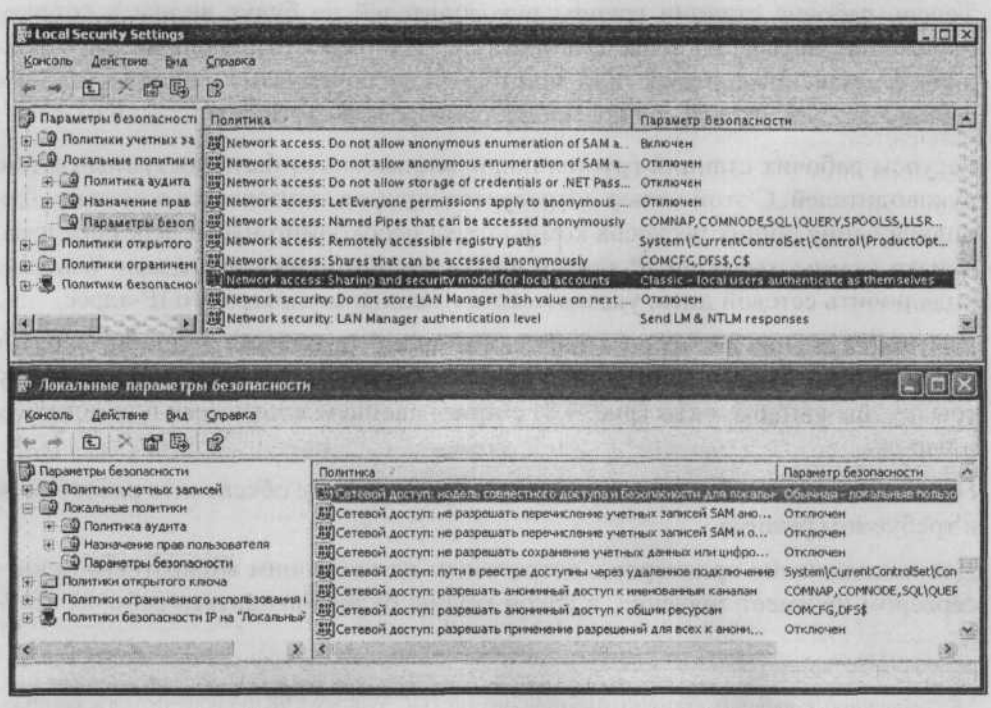

Рис. 4.6. Окно **Локальные параметры безопасности (Local Security Settings)**

- **Сетевой доступ: не разрешать перечисление учетных записей SAM (Security Accounts Manager) и общих ресурсов анонимными пользователями (Network access: Do not allow anonymous enumeration of SAM accounts and shares).**
- **Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями (Network access: Do not allow anonymous enumeration of SAM accounts).**

SAM (Security Accounts Manager) — защищенная база данных, в которой хранится информация о пользовательских учетных записях

Для первого из этих параметров следует установить значение **Классический** (Classic), а для двух других — **Отключен**.

Примечание

Описываемые настройки могут быть выполнены только на рабочих станциях Windows XP Professional.

Дополнительно на рабочих станциях группы руководителей необходимо включить учетную запись **Гость**, установив для нее пустой пароль и назначив ресурсы общего доступа.

Теперь рабочие станции группы руководителей не будут видны в сетевом окружении других рабочих станций. Но возможность использовать какой-либо разрешенный ресурс или принтер, подключенный к рабочей станции группы руководителей, будет предоставлена всем рабочим станциям сети[1].

Ресурсы рабочих станций группы подчиненных могут быть доступны группе руководителей. С этой целью потребуется лишь авторизоваться в домене. Для подключения общих ресурсов компьютеры необходимо найти через средство поиска компьютеров по IP-адресу либо стандартными средствами Windows подключить сетевой диск, указав вместо имени компьютера его IP-адрес.

Для подключения ресурсов с рабочих станций, входящих в домен, следует использовать **Подключение под другим именем** (рис. 4.7). Выбрав эту ссылку, вы увидите окно (рис. 4.8) с приглашением ввести имя пользователя и пароль.

Подключив все необходимые ресурсы и принтеры, вы обеспечите работу сети в требуемом режиме.

Для подключения принтеров с встроенным или внешним аппаратным принт-сервером не имеет значения, в какой группе будет находиться рабочая стан-

[1] К сожалению, с рабочих станций, работающих под ОС Windows 98, подключиться к компьютерам группы руководителей не удастся.

ция, с которой осуществляется подключение. У принтера в этом случае есть свой IP-адрес, по которому к нему можно подключаться, даже если этот адрес не соответствует адресу сети. Мастер установки принтеров в Windows XP позволяет настроить порт для такого принтера в интерактивном режиме, но можно это сделать, просто установив необходимые значения IP-адреса и тип порта принтера. На рисунке (рис. 4.9) показан возможный вариант настройки порта принтера с принт-сервером. Принтеры с принт-серверами от различных производителей имеют свои особенности настройки. Поэтому, приобретая такое оборудование, не теряйте дистрибутивные диски, которые к нему прилагаются, — на них могут быть утилиты, облегчающие подключение и настройку принт-серверов, смену их IP-адреса.

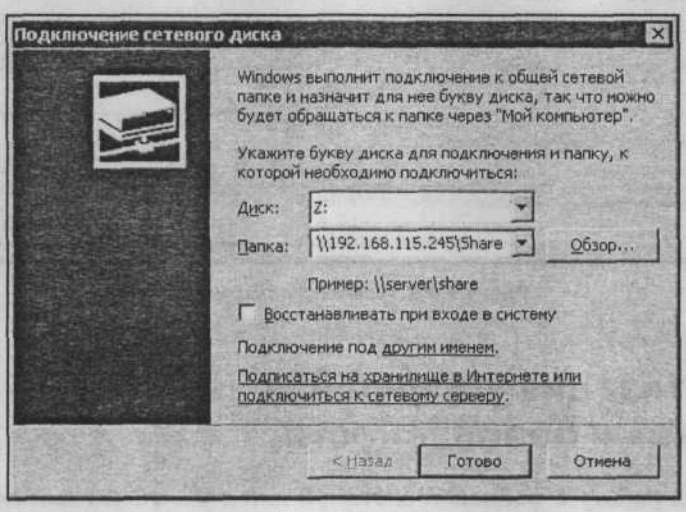

Рис. 4.7. Подключение сетевого ресурса

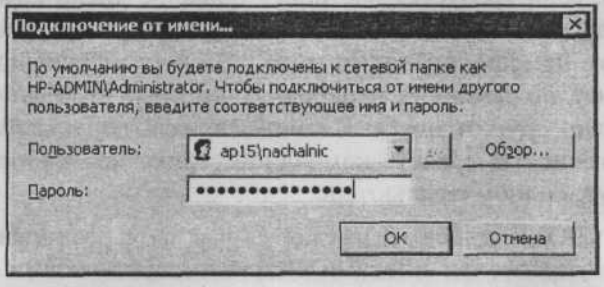

Рис. 4.8. Подключение сетевого ресурса от имени пользователя домена

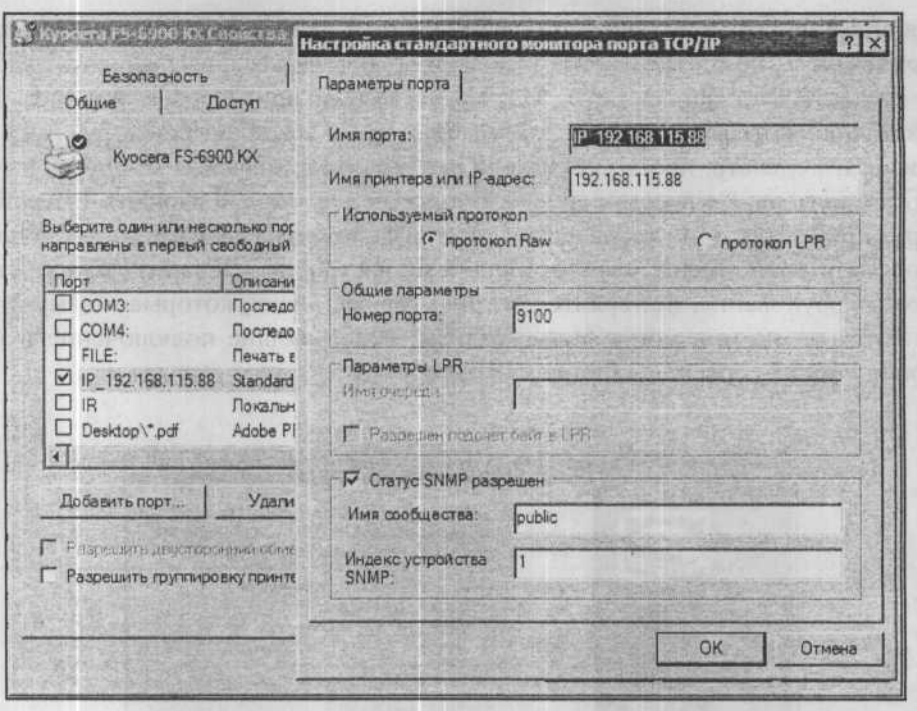

Рис. 4.9. Настройка порта принтера

Автоматизация управления политиками безопасности

Рассматривая работу с файловой системой или с учетными записями пользователей, мы стремились добиться повышения производительности и удобства работы администратора сети. Управление политиками безопасности может быть упрощено, если требуется настроить большое число компьютеров. Конечно, если надо изменить всего два параметра на трех компьютерах, находящихся в одном помещении, то это можно сделать и вручную. Другое дело, когда параметров, подлежащих изменению, много, а компьютеры находятся достаточно далеко друг от друга. В таких случаях допускается применение шаблонов безопасности, средств командной строки или работа с консолями управления на удаленном компьютере.

В папке C:\WINDOWS\system32 находятся файлы с расширением msc. Это файлы консоли управления многими объектами и службами компьютера и домена. При выборе ярлыка (пункта меню), соответствующего локальным параметрам безопасности, например, программа mmc.exe откроет файл C:\WINDOWS\system32\secpol.msc. Программа mmc.exe может быть вызвана

через стандартную операцию **Выполнить** | mmc. При этом откроется окно программы (рис. 4.10), в которое можно добавить любую оснастку для управления компьютером.

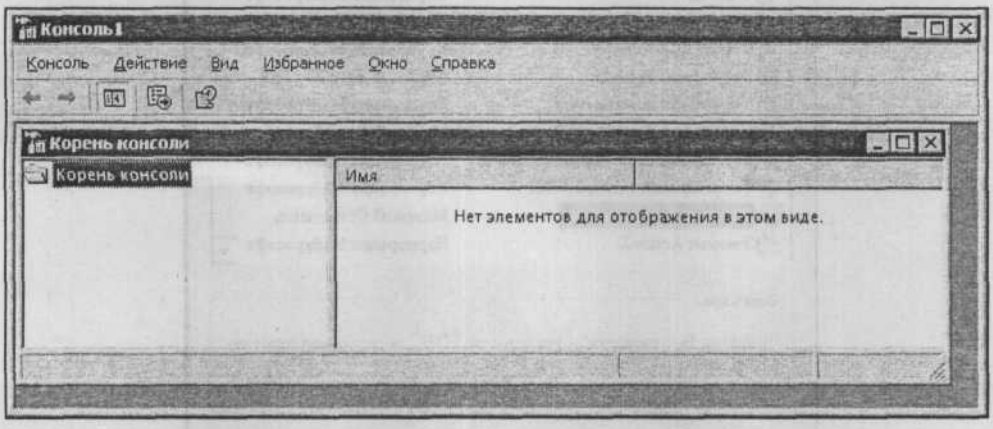

Рис. 4.10. Окно программы msc.exe

Для добавления оснастки требуется выбрать в меню **Консоль | Добавить или удалить оснастку... | Добавить**.

В открывшемся окне **Добавить изолированную оснастку** (рис. 4.11) останется выбрать из списка требуемую оснастку. Затем выбрав **Консоль | Сохранить как...** (рис. 4.10), вы можете сохранить файл консоли, настроенный по вашим предпочтениям и содержащий необходимые оснастки. Среди доступных для добавления оснасток есть такая, как **Анализ и настройка безопасности**. Эта оснастка позволяет проанализировать текущие настройки безопасности, выбрав файл базы данных, а также сохранить текущие параметры безопасности в файле шаблона (экспорт шаблона). С помощью команды **Импорт шаблона** из меню **Действие** можно изменить настройки безопасности компьютера в соответствии с импортируемым шаблоном.

Примечание

В зависимости от версии дистрибутива ОС и ее обновлений, команда **Импорт шаблона** может иметь название **Импорт политики**

При проведении анализа будет создан лог-файл, в котором перечислены все ошибки (с точки зрения ОС) в настройках безопасности. Добавив необходимые вам оснастки, вы можете сохранить получившуюся консоль под понятным вам именем и в дальнейшем использовать ее для работы. Еще одна полезная в нашем случае оснастка — **Шаблоны безопасности**. С ее помощью можно создавать и редактировать шаблоны безопасности.

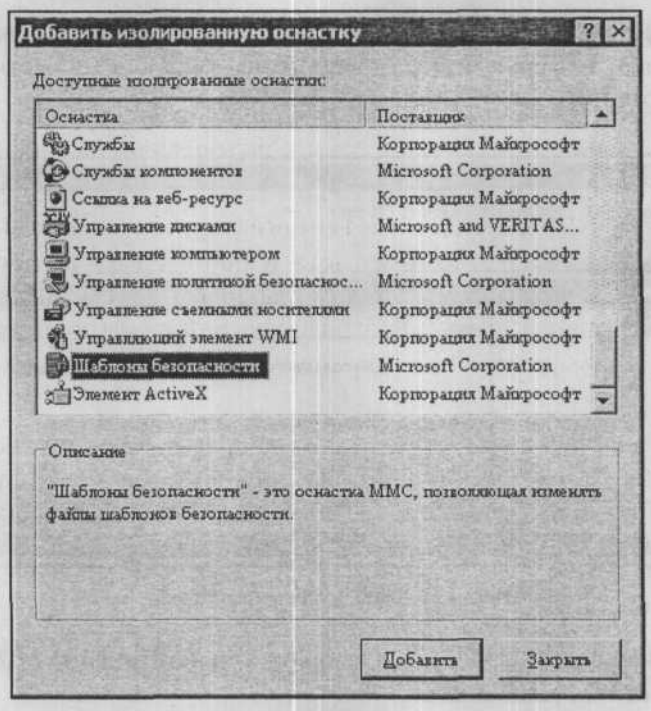

Рис. 4.11. Окно **Добавить изолированную оснастку**

Их можно использовать для изменения конфигурации одного или нескольких компьютеров. Изменение конфигурации компьютеров допустимо при помощи оснастки **Анализ и настройка безопасности** средства Secedit.exe, работающего из командной строки, а также при помощи импорта шаблона в оснастку **Локальная политика безопасности**. По умолчанию готовые шаблоны безопасности сохранены по адресу: системный_корневой_каталог\Security \Templates.

Поле установки ОС в системе могут присутствовать приведенные далее шаблоны.

- **Setup security.inf — "шаблон безопасности по умолчанию"**, содержит параметры безопасности, используемые по умолчанию, которые применяются во время установки операционной системы, включая разрешения для файлов корневого каталога системного диска. Этот шаблон можно использовать полностью или частично в целях аварийного восстановления.
- **Compatws.inf — "совместимый"**, содержит разрешения по умолчанию для рабочих станций и серверов (не контроллеров домена). Учитывается иерархия прав локальных групп: "Администраторы", "Опытные пользователи" и "Пользователи".

- **Secure*.inf — группа шаблонов "защита"**, содержит параметры повышенной безопасности.
- **Hisec*.inf — группа шаблонов "повышенная защита"**, включает в себя шаблоны, налагающие дополнительные ограничения на уровни кодировки и подписи.
- **Rootsec.inf — "безопасность системного корневого каталога"**, включает разрешения для корневого каталога Windows XP Professional. По умолчанию эти разрешения определяются шаблоном Rootsec.inf для корневого каталога системного диска. Шаблон также может быть изменен для применения этих разрешений к корневому каталогу других дисков (не системных).

Параметры шаблонов безопасности можно просмотреть и отредактировать при помощи компонента **Шаблоны безопасности**. Причем их редактирование аналогично редактированию реальных параметров безопасности. Файлы шаблонов с расширением inf можно просматривать как текстовые файлы.

> ***Примечание***
>
> Обеспечение безопасности невозможно в системах Windows XP Professional, установленных на дисках с файловой системой FAT.

Выбрав наиболее подходящий шаблон или создав новый, можно внести в него необходимые изменения и распространить их на другие компьютеры, не проводя редактирования параметров безопасности на каждом компьютере отдельно.

Чтобы создать новый шаблон, достаточно в окне созданной консоли выбрать в контекстном меню папки, содержащей шаблоны (рис. 4.12), опцию **Создать новый шаблон**, дать ему имя и добавить описание.

Для настройки безопасности системы с использованием сохраненного шаблона можно применить пакетные (командные) файлы с заготовленными заранее командами, включающие представленные в листинге 4.7 строки.

Листинг 4.7. secedit.bat

```
secedit /configure /db C:\WINDOWS\security\Database\abcd.sdb /cfg
c:\WINDOWS\security\templates\new.inf
pause
```

где:

- `secedit` — средство командной строки для редактирования параметров безопасности;

- `abcd.sdb` — имя базы данных, которая будет создана в процессе выполнения команды;
- `new.inf` — примененный шаблон безопасности.

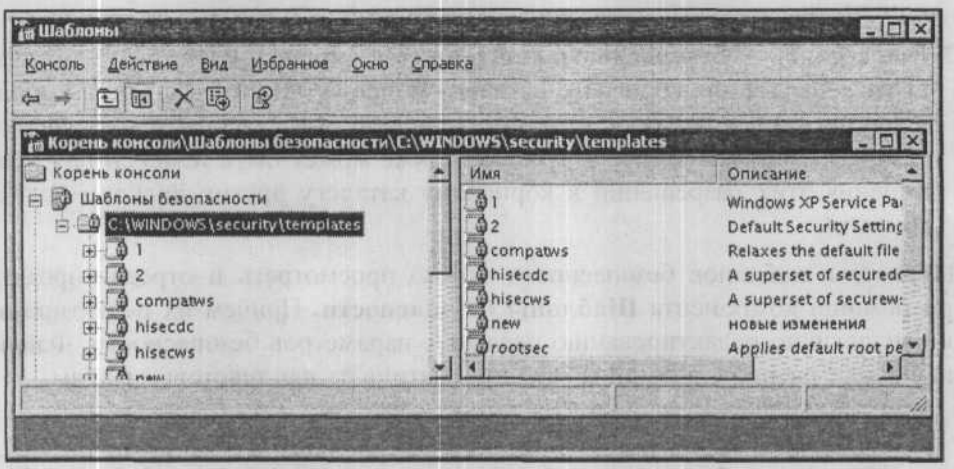

Рис. 4.12. Список шаблонов безопасности

После выполнения такого пакетного файла все определенные в шаблоне new.inf политики будут применены на компьютере, а все параметры, не определенные в шаблоне, но используемые в настройках компьютера, останутся без изменений.

Применив этот способ распространения политик безопасности, вы можете передать все необходимые изменения настроек компьютерам группы руководителей, рассмотренной ранее в этой главе.

Возможности программ Secedit и mmc существенно шире, чем те, что показаны в примерах. Если вы внимательно прочтете встроенную в систему справку по работе с этими программами, то сможете проводить анализ настроек безопасности, а также редактировать групповую политику безопасности, применяемую в домене. Политики и параметры безопасности, определенные на уровне домена, имеют преимущество перед политиками и параметрами, определенными локально.

Здесь же остается добавить только, что все операции должны выполняться от имени администратора компьютера или домена. Как и в других случаях администрирования сети, ошибка, допущенная вами, может потребовать продолжительного времени на исправление. Будьте внимательны!

Управление доступом к некоторым объектам сети

Обычно, когда уровень доступа к объектам сети определяется только разрешениями в сети, не возникает проблем с нарушением режима доступа к информации. Но в отдельных случаях режим доступа определяется средствами приложений, в которых работают пользователи. Например, весьма распространены приложения, разработанные в среде MS Access. Для работы в сети эти приложения делятся на клиентскую и серверную части. Клиентская часть распространяется между пользователями, а серверная расположена на сервере. Определяя режим доступа к данным, устанавливают пароли для доступа к определенным частям приложения, соответствующим профилю работы пользователей. В MS Access для управления паролями применяют файл рабочих групп. При обычной работе пользователей информация достаточно хорошо защищена от изменения, а возможно и просмотра теми пользователями, которым не дано на это право в приложении.

В то же время продвинутые пользователи, желая подсмотреть или скорректировать информацию, к которой они не должны иметь доступа, могут это сделать, подключившись к серверной базе данных и используя стандартные или разработанные самостоятельно средства. Конечно, приложения, которые создаются фирмами, специализирующимися на разработке клиент-серверных продуктов, снабжаются достаточно эффективными средствами защиты данных. В простых разработках, созданных зачастую самими администраторами сети или другими сотрудниками предприятия, вопрос защиты серверной базы данных нередко упускается из виду. Для упрощения организации работы новых пользователей с клиентскими приложениями доступ к серверной базе данных открывается для всех пользователей домена. Тем не менее вопрос защиты серверной базы данных может быть решен на уровне файловой системы. Достаточно определить доступ к каталогам, в которых размещены файлы базы данных, лишь для пользователей этой базы данных, причем в той степени, в которой это необходимо.

Разрешения для каталога задаются стандартными средствами операционной системы. Существуют два варианта определения доступа. Каталог может быть виден в сетевом окружении или же доступен при открытии содержащего его каталога после подключения к компьютеру из сети. Как будет организован доступ к каталогу, зависит от условий работы ваших пользователей и требований программного обеспечения. Кроме того, полноценное управление разрешениями возможно лишь при наличии на сервере файловой системы NTFS. Добавлять и удалять разрешения для отдельных пользователей — задача достаточно трудоемкая. Поэтому, как и в большинстве случаев управления доступом, рациональнее создать группы пользователей с установленны-

ми правами, а при необходимости добавлять в них учетные записи пользователей. Средства, необходимые для этого, мы уже рассматривали ранее.

Кроме описанных вариантов защиты информации серверной базы данных MS Access, не считая встроенной возможности установки пароля на открытие базы, можно применить небольшой модуль, запрещающий случайное прямое открытие базы пользователем, не имеющим на это права. Модуль должен вызываться из формы, которая не содержит ничего, кроме одного модуля формы (листинг 4.8), из которого и запускается модуль InTo (листинг 4.9). Имя формы должно быть внесено в поле **Форма** в параметрах запуска базы данных.

Листинг 4.8. Модуль формы Start

```
Private Sub Form_Open(Cancel As Integer)
InTo.VXOD
DoCmd.Close
End Sub
```

Листинг 4.9. Модуль InTo

```
Option Compare Database
Option Explicit
Public Sub VXOD()

Dim UserIN As String
 UserIN = Left(DBEngine.Workspaces(0).UserName, 15)
 MsgBox UserIN
If UserIN <> "Fedor" Then
    DoCmd.Quit
End If

End Sub
```

Если для работы с базой применяется файл рабочей группы, то только пользователь `Fedor` сможет открыть ее.

Конечно, знатоки MS Access уже приготовили усмешку и возражение: мол, знаем же простой путь обхода этой защиты... Разумеется, предложена защита от *случайного* открытия и случайной порчи базы данных, когда другие средства защиты не применяются или не применимы. Кроме того, дополнительные возможности защиты в арсенале администратора лишними не будут.

Доступ к очередям печати и управлению ими

Один из специфических объектов в сети, доступ к которому может иметь администратор и отдельные доверенные пользователи, — это очередь печати. В зависимости от того, как организована в вашей сети печать, эти функции администрирования могут быть необходимы в разной степени. Например, если в сети применяются только аппаратные (например, встроенные в принтеры) принт-серверы, и рабочие станции настроены таким образом, что документы отправляются непосредственно на принт-сервер, минуя сервер сети, то администрирование процесса печати не требуется. В то же время при ограниченном числе принтеров, но большом объеме печати, возможны проблемы со своевременной заправкой принтеров бумагой и тонером. Очень большое число документов в очереди на один принтер может привести к "зависанию" принт-сервера. В таких случаях желательно процесс печати контролировать и управлять им. Для успешного управления большим объемом сетевой печати очереди должны находиться на одном или двух (если объем печати очень большой) расположенных рядом компьютерах. Это позволит оператору печати эффективно управлять очередями, при необходимости вмешиваясь в процесс печати документов. Для помещения всех очередей печати на один компьютер, например сервер, нет необходимости все принтеры подключать к нему физически. Достаточно установить их как сетевые, но разрешить к ним доступ пользователей, настроив соответствующим образом рабочие станции.

На рабочей станции достаточно найти необходимый принтер в сетевом окружении, установленный на сервере, и выбрать в контекстном меню команду **Подключить**. В перечне установленных принтеров в папке **Принтеры** появится еще один принтер. При выборе принтера для отправки документа на печать установленные таким образом принтеры будут выглядеть, как сетевые, например **\\Ap15nt01\Kyocera FS-6900** (рис. 4.13). Тот же принт-сервер, но с локальной очередью печати, подключенный через стандартный IP-порт (см. рис. 4.9), выглядит как локально подключенный принтер **Kyocera FS-6900 KX**.

> ***Примечание***
>
> Различие в названиях принтера связано с применением разных драйверов при локальной и сетевой установке. Это может быть удобно при различных вариантах печати.

Если на рабочих станциях, с которых идет большой объем печати, применять только сетевую установку принтера, то очередь печати будет находиться на сервере, через который принтер подключен к рабочей станции.

Открыв окно очереди печати принтера (рис. 4.14), можно контролировать ход печати, приостанавливать отдельные задания большого объема, удалять оши-

бочные и повторные, перезапускать задания, пользуясь контекстным меню каждого из них.

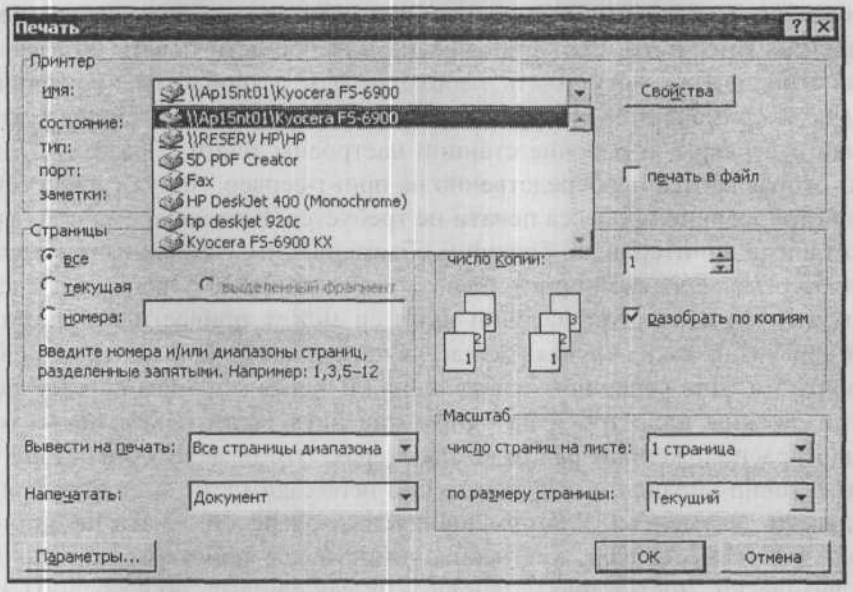

Рис. 4.13. Выбор принтера в окне **Печать**

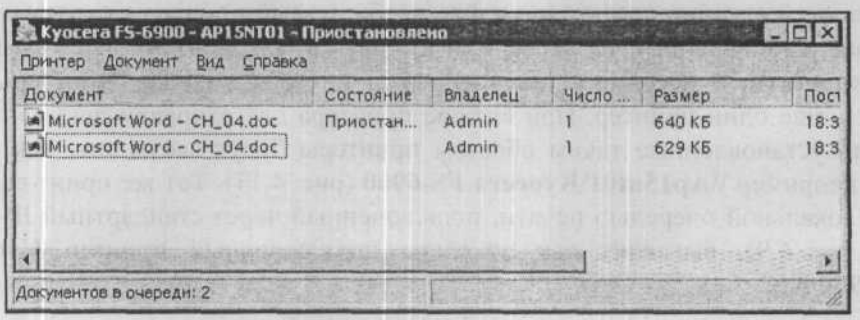

Рис. 4.14. Окно очереди печати принтера

При необходимости можно приостановить всю очередь для проведения работ с принтером, а после их завершения запустить печать снова.

Доступ к принтерам, права на изменение режима печати, управление очередью печати, права на саму печать можно задавать в свойствах принтера на вкладке **Безопасность** (рис. 4.15).

В серверных ОС предусмотрена специальная группа **Операторы печати** (рис. 4.16). Пользователи, включенные в эту группу, будут иметь права

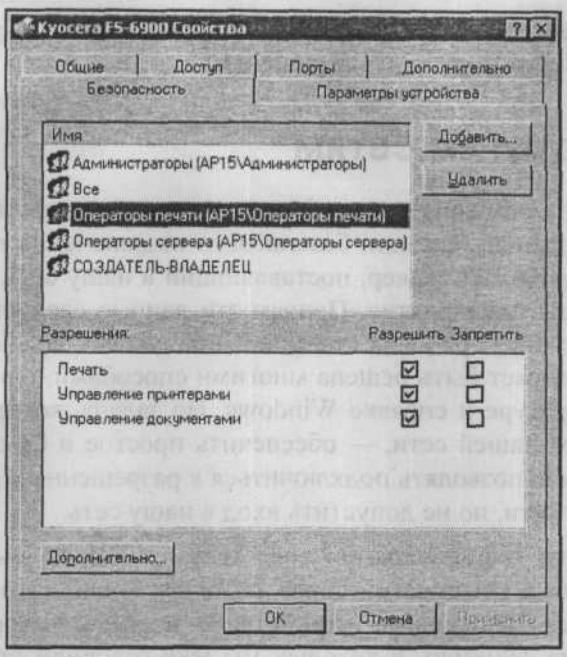

Рис. 4.15. Окно свойства принтера, вкладка **Безопасность**

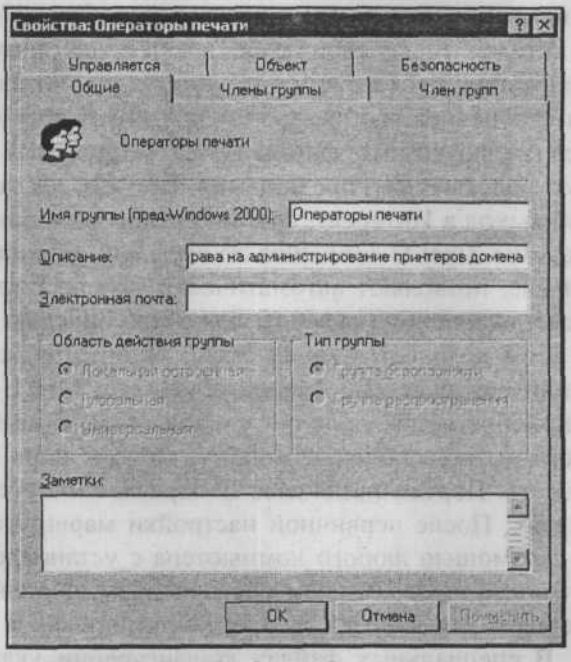

Рис. 4.16. Окно **Свойства: Операторы печати**

управления процессом печати на любом принтере домена. Другие права этих пользователей в сети могут быть ограничены.

Доступ к другим сетям

В данном разделе опишем, не углубляясь в отдельные частные вопросы настройки оборудования, принцип безопасного подключения к некой внешней сети, в которой работает сервер, поставляющий в нашу сеть данные, необходимые для работы предприятия. Причем эти данные следует получать лишь на ограниченном числе рабочих станций. Сама по себе задача подключения к удаленной сети может быть решена многими способами, описанными в компьютерной литературе и справке Windows. Но задача, которая стояла перед администратором нашей сети, — обеспечить простое и безопасное подключение. Оно должно позволять подключиться к разрешенным ресурсам на сервере во внешней сети, но не допустить вход в нашу сеть.

Вопрос настройки маршрутизации средствами Windows мы рассматривали при подключении к Интернету в *главе 2*. Теперь коснемся организации маршрутизации через специальные устройства — маршрутизаторы. По сути, они выполняют те же функции, о которых мы уже говорили при рассмотрении настроек маршрутизации и удаленного доступа на сервере. Но настройка для всех этих устройств не может быть описана единообразно. Устройства различных производителей имеют свои особенности и свои интерфейсы настроек и администрирования. Часто к ним требуются дополнительные платы расширения, чтобы обеспечить работу по тем или иным протоколам. В нашей сети применяется маршрутизатор фирмы Allied Telesyn AR410 для обеспечения связи с сетью родственного предприятия. Причем, несмотря на то, что у нас есть удобный выход в Интернет, связь по некоторым причинам осуществляется через модемы Zixel U-336E Plus по выделенной линии. Эти модемы, как и многие другие, позволяют автоматически устанавливать связь модем-модем сразу после включения (команды для этого описаны в документации на модем). При этом появляется канал связи, который можно использовать для маршрутизации между сетями. Маршрутизатор AR410 с помощью платы AT-AR024-00 (приобретается дополнительно), обеспечивающей работу с асинхронным портом, подключен к модему. Другой порт маршрутизатора включен в нашу сеть. Портам назначены IP-адреса, соответствующие допустимым в двух сетях. После первичной настройки маршрутизатора, которая осуществляется с помощью любого компьютера с установленным прилагаемым к маршрутизатору программным обеспечением, подключаемого к маршрутизатору специальным кабелем, его администрирование возможно через Web-интерфейс. В специальных файлах конфигурации указываются имена пользователей, их полномочия и пароли. Подключаясь через Web-интерфейс

к маршрутизатору, необходимо авторизоваться. Кроме Web-интерфейса, для управления маршрутизатором можно применять Telnet. Открыв соответствующие порты для доступа из Интернета и перенаправив их на адрес маршрутизатора средствами NAT, можно получить доступ к управлению им из Интернета. При попытке подключения через Web-интерфейс вам будет предложено авторизоваться (рис. 4.17).

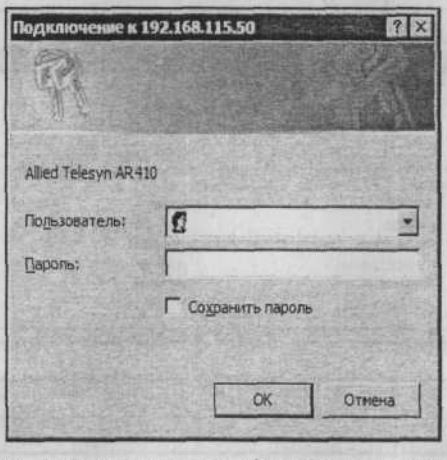

Рис. 4.17. Окно **Подключение к [Адрес маршрутизатора]**

После авторизации будет представлено главное окно с информацией о маршрутизаторе (рис. 4.18), в котором с помощью обычного для интернет-браузера меню можно получить доступ ко всем настройкам этого маршрутизатора.

На рис. 4.19 показано окно редактора файлов конфигурации с фрагментом раздела IP configuration, где описаны все необходимые маршруты.

Характеристика необходимых команд и их синтаксис приведены в описании маршрутизатора на прилагаемом к нему CD. При необходимости можно удаленно перезагрузить маршрутизатор, пользуясь Web-интерфейсом или утилитой Telnet (рис. 4.20).

Показанное на рис. 4.20 окно позволяет убедиться в том, что маршрутизатор включен и все необходимые соединения установлены.

Теперь рассмотрим суть способа обеспечения безопасности подключения.

Обеспечение безопасности на стороне внешней сети, — задача ее администратора, поэтому рассмотрим решение задачи только с одной стороны.

На рис. 4.21 схематически показана организация подключения к внешней сети.

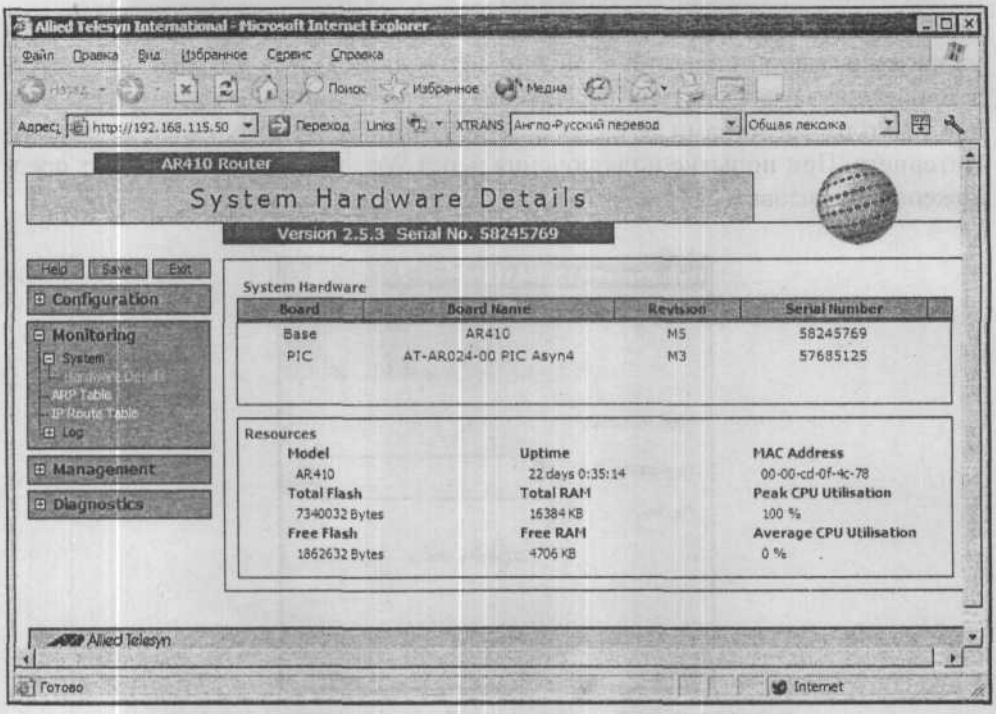

Рис. 4.18. Окно управления маршрутизатором через Web-интерфейс **Allied Telesyn International**

Если во внутреннюю сеть обеспечен доступ из внешней сети, то существует вероятность того, что ресурсы внутренней сети, доступные для всех ее пользователей, будут доступны и для случайного пользователя внешней сети. В нашем случае требовалось исключить такую возможность, но не усложнять политику доступа к ресурсам внутри сети.

Для ограничения доступа к ресурсам сети было использовано свойство IP-адресов в сетях — маска подсети, а также невозможность прямого подключения к компьютерам сети, к которым не указаны явно маршруты.

На рис. 4.19 показано окно с фрагментом содержания файла IP-настроек маршрутизатора, в котором описаны сети и адреса, допустимые для подключения. Выберем из всех строк только те, что касаются решения поставленной задачи. Знаком "#" обозначим комментарии, которые не обязательны в файле конфигурации и не используются маршрутизатором. Реально эти комментарии могут отсутствовать в файле, здесь же они приведены для разъяснения назначения строк. Описываемая часть файла конфигурации показана в листинге 4.10.

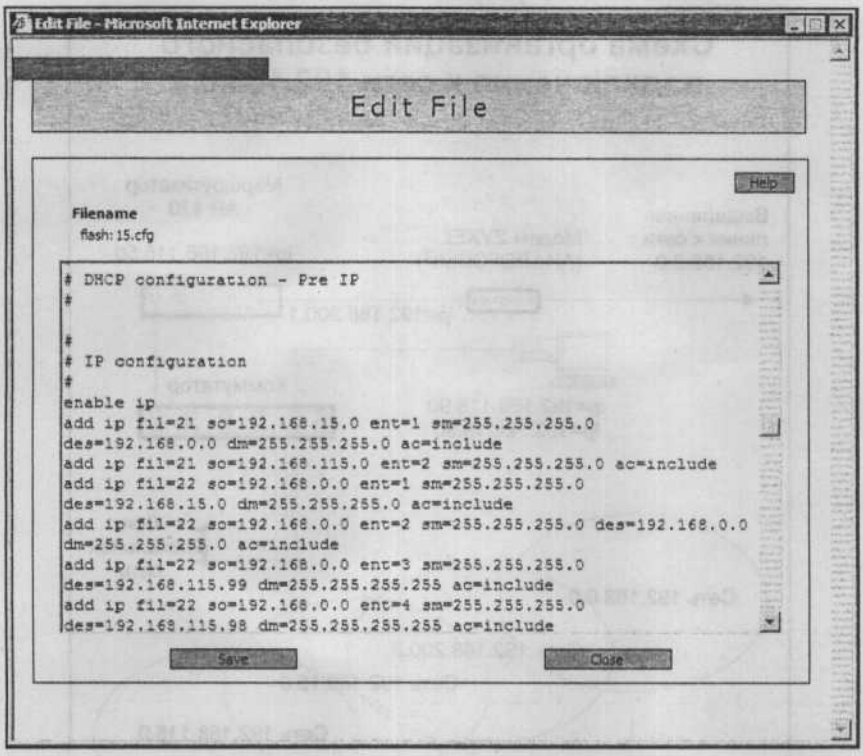

Рис. 4.19. Окно **Edit File**

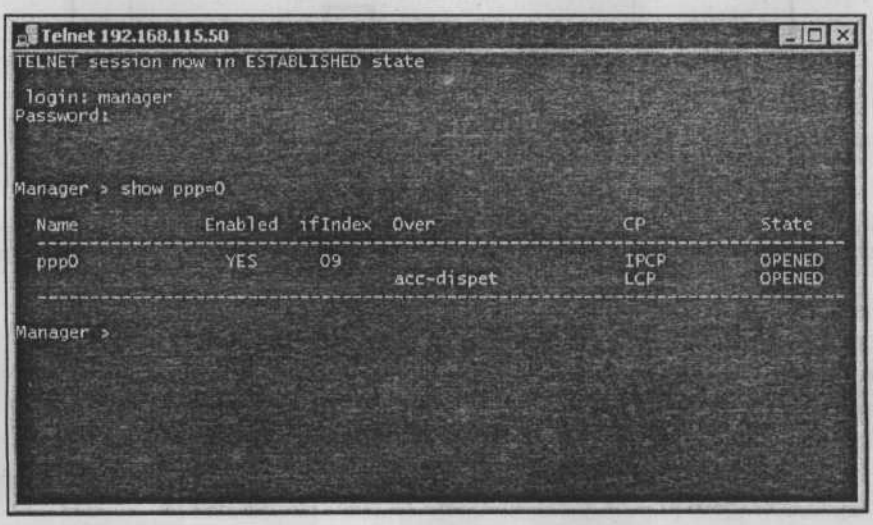

Рис. 4.20. Окно **Telnet** сеанса связи с маршрутизатором

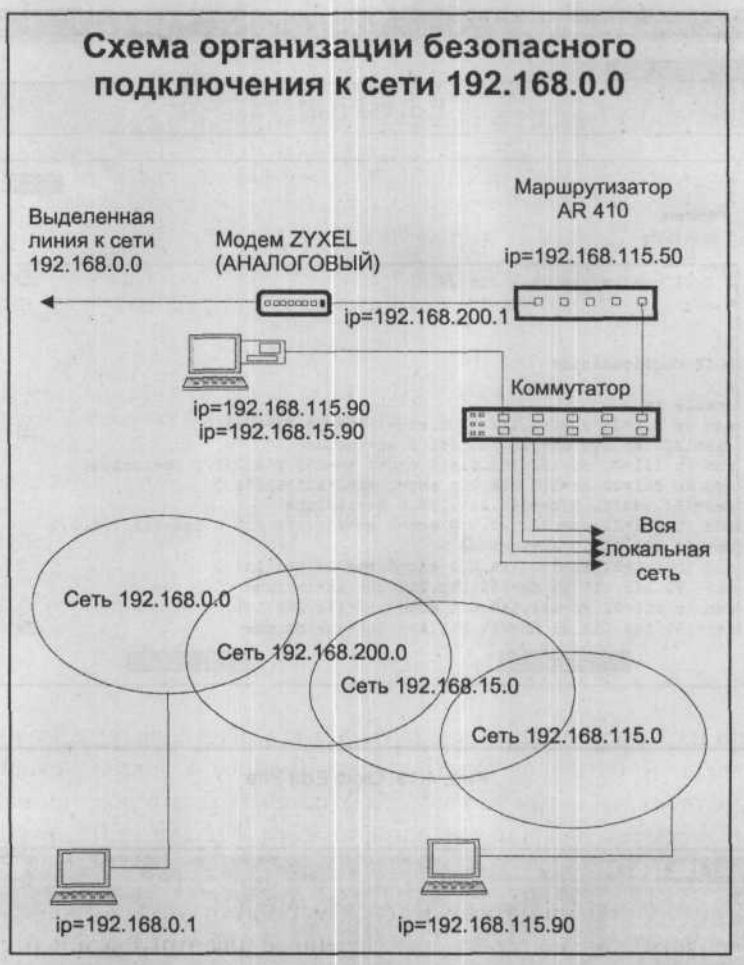

Рис. 4.21. Схема организации безопасного подключения к сети 192.168.0.0

Листинг 4.10. Фрагмент файла конфигурации маршрутизатора

```
# – разрешение сети 192.168.15.0 подключаться к сети 192.168.0.0
add ip fil=21 so=192.168.15.0 ent=1 sm=255.255.255.0 ↳
des=192.168.0.0 dm=255.255.255.0 ac=include
# – разрешение сети 192.168.115.0 подключаться к сети 192.168.0.0
add ip fil=21 so=192.168.115.0 ent=2 sm=255.255.255.0 ac=include
# – разрешение сети 192.168.0.0 подключаться к сети 192.168.15.0
add ip fil=22 so=192.168.0.0 ent=1 sm=255.255.255.0 ↳
des=192.168.15.0 dm=255.255.255.0 ac=include
```

```
# - разрешение сети 192.168.0.0 подключаться к сети, состоящей
из единственного адреса - 192.168.115.99
add ip fil=22 so=192.168.0.0 ent=3 sm=255.255.255.0 ↳
des=192.168.115.99 dm=255.255.255.255 ac=include
# - разрешение сети 192.168.0.0 подключаться к сети, состоящей
из единственного адреса - 192.168.115.98 (фактически, - разрешение
компьютеру 192.168.115.98 получать информацию из сети 192.168.0.0)
add ip fil=22 so=192.168.0.0 ent=4 sm=255.255.255.0 ↳
des=192.168.115.98 dm=255.255.255.255 ac=include
# - назначение порту маршрутизатора, смотрящему во внутреннюю сеть,
адреса 192.168.115.50
add ip int=vlan3 ip=192.168.115.50 fil=21
# - назначение порту маршрутизатора, смотрящему во внешнюю сеть, адреса
192.168.200.1 (по договоренности с администратором внешней сети)
add ip int=ppp0 ip=192.168.200.1 fil=22
# - назначение маршрута в сеть 192.168.0.0 на адрес 192.168.0.20
(по договоренности с администратором внешней сети)
add ip rou=192.168.0.0 mask=255.255.255.0 int=ppp0 next=192.168.0.20
# - назначение маршрута в сеть 192.168.15.0 на любой ее адрес
add ip rou=192.168.15.0 mask=255.255.255.0 int=vlan3 next=0.0.0.0
# - указание адреса DBS-сервера
add ip dns prim=192.168.115.15
```

Выполнено назначение сетевым адаптерам компьютеров, участвующих в общении с внешней сетью, дополнительных IP-адресов, принадлежащих реально не существующей сети 192.168.15.0. У сетевых адаптеров, принадлежащих этой сети, имеются два адреса: один из сети 192.168.15.0, другой из сети 192.168.115.0.

В результате применения этих настроек маршрутизатор позволяет из внешней сети "видеть" только строго определенные для этого компьютеры нашей сети (и то по дополнительным IP-адресам). Вход в сеть 192.168.115.0 для пользователя внешней сети невозможен (некоторые адреса этой сети выделены для доступа из внешней сети, как отдельные сети).

Учитывая необходимость авторизации в домене для доступа к ресурсам сети, доступ в нашу сеть из внешней сети практически невозможен. Доступ из нашей сети во внешнюю обеспечен частично, а именно к разрешенным для этого администратором внешней сети ресурсам. С этой целью используется компьютер, не входящий в домен внешней сети, что позволяет, как мы уже рассмотрели в *разд. "Изолированные" подсети" этой главы*, обеспечить к нему доступ из любой внешней сети. Для этого необходимо лишь установить соответствующие разрешения.

Разумеется, безопасность подключения к внешней сети обеспечена не только собственно маршрутизацией и организацией специфического адресного про-

странства. Важны и другие компоненты защиты, такие как сложные пароли для доступа к настройкам маршрутизатора по telnet-протоколу или через Web-интерфейс.

Возможно, что в вашем случае будет реализован иной способ маршрутизации, например, путем применения дополнительного компьютера с серверной операционной системой. Но использование описанного принципа безопасной связи с другой сетью возможно в любом варианте реализации маршрутизации.

Виртуальный компьютер и виртуальная сеть

Несколько забегая вперед, рассмотрим вариант доступа к отдельным ресурсам сети с помощью программ, которые будут описаны в *главе 6*. Там будет приведено описание программы Microsoft Virtual PC, которая позволяет организовать на реальном компьютере еще один — виртуальный; и программы OpenVPN, позволяющей создать виртуальную сеть. Читая в *главе 6* описание названных программ, вы уже будете представлять, зачем они вам нужны.

В ряде случаев доступ к отдельным ресурсам сети или к ресурсам вне ее должен быть организован таким образом, чтобы некий пользователь не имел возможности получить доступ к другим ресурсам сети, а другие пользователи этой сети не могли получить доступ к компьютеру, для которого организован такой специальный доступ. Задача напоминает ту, что рассматривалась выше, когда разговор шел об изолированных подсетях. Но в данном случае речь идет о доступе, который допустимо организовать даже через Интернет, а информация, передаваемая по сети, не может быть перехвачена и прочитана. Здесь мы рассмотрим пример общей схемы организации такого доступа. Подробности для решения конкретных задач описаны в *главе 6*.

Суть решения заключается в том, что можно организовать виртуальную сеть, состоящую как из реальных, так и из виртуальных компьютеров, которая физически может быть частью вашей сети или же выходить за ее пределы, как бы пересекаясь с ней. При этом система адресов и способ идентификации компьютеров несколько отличается от того, что применяется в обычной сети. В обычной сети рабочие станции и сервер "узнают" друг друга по IP-адресам, именам и принадлежности к домену или рабочей группе. Доступ к ресурсам сети и к компьютерам определяется политиками доступа, существующими в сети. Виртуальная сеть имеет в своем распоряжении дополнительные средства идентификации и ограничения доступа, перечисленные ниже:

- каждый компьютер такой сети может быть сервером и/или клиентом виртуальной сети;

- каждая пара или большая группа компьютеров виртуальной сети может иметь общий секретный ключ доступа;
- доступ к компьютерам может быть определен не только адресом, но портом (подобно тому, как к Web-серверу можно обращаться по разным портам, попадая на разные страницы сайта);
- сами компьютеры могут быть как реальными, так и виртуальными;
- виртуальные компьютеры могут находиться на реальных машинах как принадлежащих одной из сетей, так и не принадлежащих им;
- на каждом компьютере может находиться несколько виртуальных адаптеров, каждый из которых обеспечивает связь с определенным VPN-сервером или клиентом.

Строя виртуальную сеть, вы можете обеспечить абсолютную конфиденциальность связи внутри любой группы компьютеров.

Практически невероятно, чтобы посторонний смог перехватить информацию, которой обмениваются машины в виртуальной сети, основанной на VPN (Virtual Private Network, виртуальная частная сеть). Этой устойчивостью виртуальных сетей к взлому в последнее время широко пользуются организаторы районных или городских сетей, предоставляя пользователям доступ в Интернет.

Если вы имеете такой доступ в Интернет дома, то можете через существующий VPN-канал в Интернете проложить свой VPN-канал к вашей локальной сети. При таком варианте связи вы будете защищены от любых попыток перехвата паролей и данных, которыми вы обмениваетесь с вашей сетью. Обычно опасность перехвата паролей существует в сеансах Telnet, где пароли передаются в открытом виде при авторизации на почтовых серверах, а также в других случаях, когда пароли пересылаются в открытом виде. Обмен данными внутри локальной сети также становится безопасным, если применяется защищенный VPN-канал.

На рис. 4.22 показан вариант организации виртуальной сети с применением виртуальных компьютеров. Виртуальные компьютеры имеют букву "V" на экране монитора, как и виртуальные сетевые адаптеры, которые необходимы для работы виртуальной сети. Светлые стрелки обозначают связи между компьютерами в виртуальной сети. Виртуальные компьютеры, конечно, находятся на реальных машинах, но ведут они себя так, как если бы были самостоятельными компьютерами. Виртуальные связи между машинами показаны таким образом, как будто они не требуют физических линий связи. Именно так они будут восприниматься пользователями компьютеров. Например, рабочая станция, находящаяся вне локальной сети и связанная с ней по виртуальному каналу через Интернет, реально связана через физические линии

связи и коммуникационное оборудование, но после установления виртуальной связи вся физическая сеть становится несуществующей для пользователя. Даже команда tracert [ip-адрес], выводящая на экран командной строки информацию о маршруте соединения, не покажет ни одного промежуточного узла между машинами, работающими в виртуальной сети. Количество виртуальных сетевых адаптеров, которые допускается устанавливать на одной машине, может быть ограничено особенностями конфигурации конкретного компьютера и системы. Но в большинстве случаев вам не потребуется более двух-трех адаптеров. С таким числом сетевых плат может нормально работать любой современный компьютер.

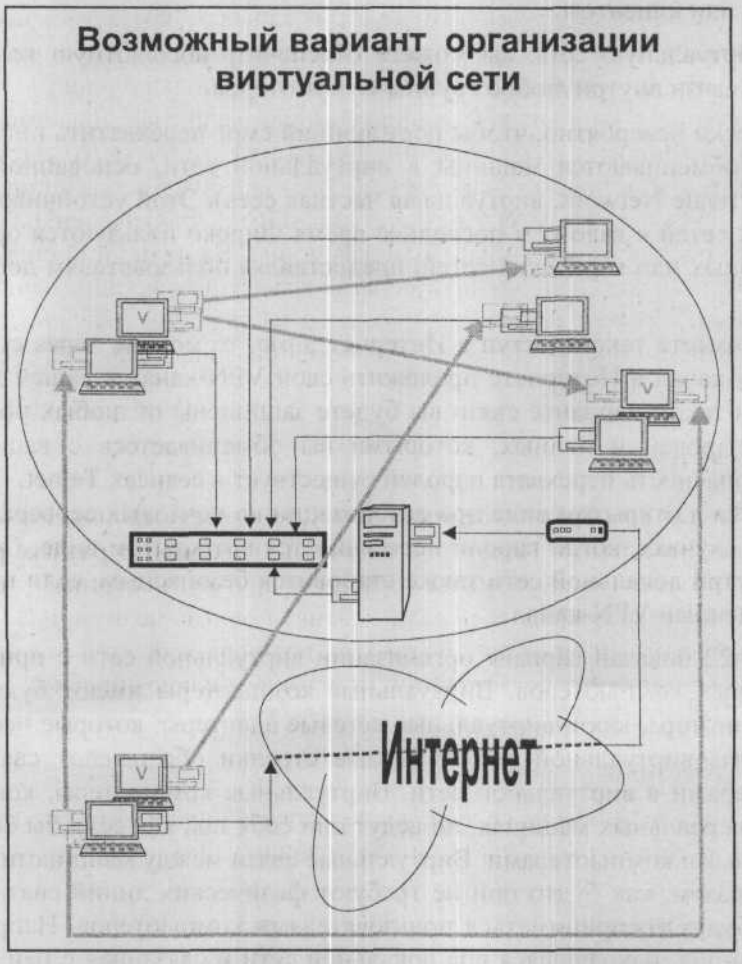

Рис. 4.22. Вариант организации виртуальной сети

Как и в реальной сети, при построении виртуальной необходимо соблюдать уникальность IP-адресов, а на каждом компьютере — и номеров портов, через которые устанавливаются соединения. Дело, правда, облегчается тем, что число виртуальных связей существенно меньше, чем реальных, а маска виртуальной подсети отличается от маски реальной подсети. В реальной сети необходимо обеспечить маршруты для портов, применяемых в виртуальных соединениях извне. Эти маршруты устанавливаются для реальных адресов машин.

Не стоит забывать о защите

Говоря о доступе к ресурсам сети, не стоит забывать и о возможности доступа к ним абсолютно посторонних, нежданных гостей. Особенно важно это учитывать при наличии постоянно работающего подключения к Интернету. Если вы поищете в поисковой машине Google, например, информацию о несанкционированном доступе к компьютерам из Интернета, то сможете обнаружить, что эти вопросы очень серьезно обсуждаются как защищающимися от такого доступа, так и его осуществляющими. Фактически на просторах Интернета идет постоянная партизанская война. Начинающий системный администратор может недооценить серьезность существующего положения и не предусмотреть мер защиты от нападения на его сеть снаружи. Даже защитив передаваемую через Интернет информацию шифрованием, следует помнить и об общей защите.

Злые хакеры

Я еще не успел разобрать утреннюю почту, как мне позвонил знакомый системный администратор. Некоторое время мы говорили о разных разностях: политике, перспективах развития отрасли и других "насущных" проблемах. При этом мне становилось все менее и менее понятна цель звонка. Мы редко с этим человеком говорим просто так. Но, наконец, все встало на свои места. После некоторой паузы позвонивший многозначительно спросил:

— А ты знаешь, что у нас произошло?

— Нет, — ответил я.

— Кто-то проник к нам на сервер, воспользовался нашим трафиком, и теперь провайдер требует, чтобы мы установили защиту. Ты не подскажешь, какую защиту лучше поставить?

— Глухую, — ответил я.

— Мы работали несколько месяцев с нашим ADSL, и ничего не происходило, а тут вдруг...

— А провайдер, — попытался пошутить я, — не установил никакой защиты в своей сети.

— В том то и дело, — оживился собеседник, — а теперь требует, чтобы установили защиту мы!

— Это, конечно, безобразие..., а что, у вас все это время ADSL был включен прямо в сеть?

— Нет, он подключен к моему компьютеру. А у тебя не так?

— Знаешь, я не люблю быть зависимым от кого бы то ни было и не хочу, чтобы зависели от меня. Поэтому я использую для выхода в Интернет отдельный сервер. Можно, конечно, поставить и аппаратный маршрутизатор со встроенным firewall и DHCP. Но так уж исторически сложилось, что Интернет у нас подключен через второй сервер. На нем и почтовый сервер, и некоторые другие службы. Сервер может работать круглосуточно, а свой компьютер я часто забираю с собой, — у меня ноутбук.

— И ты не выключаешь сервер на ночь?

— А зачем? Ночью и Интернет работает, и почта.

— А вдруг хакеры?

— Не думаю. Прежде чем подключить сервер к сети, мы намеренно пытались влезть в него из Интернета. Когда увидели, что это очень сложно, — подключили сервер, дали доступ в Интернет пользователям сети и перенесли на него почтовый сервер. А тот доступ, что необходим, осуществляется достаточно надежными средствами.

— А кто у вас разбирает приходящую почту?

— Никто. Точнее, тот, кому она адресована.

— А как же, если директору письмо придет?

— Значит, директор и разберет. Каждый имеет свой адрес. Те же адреса и внутри сети применяем.

— А как у тебя защищен сервер? Программно?

— В общем да. Только я ничего не приобретал, кроме Windows Server 2003, для защиты сервера. В нем есть почти все, что может потребоваться в небольшой сети.

— Да, но мне некуда его установить.

— А сервер, который ты хотел использовать в качестве горячего резерва?

— Он лежит на складе холодным резервом. Не получилось настроить репликацию так, как я хотел, и его выключили пока.

— Так используй его.

— Надо подумать. Но ты сказал, что есть аппаратные средства защиты сети. Что лучше применить?

— Я думаю, это дело вкуса. Конечно, аппаратные средства в целом дешевле компьютера и операционной системы, но когда уже есть компьютер, который можно применить для этих целей, почему бы и не использовать его?

— Мне кажется, что программные средства менее надежны, чем аппаратные.

— Думаю, что это не совсем так. Аппаратные средства так же, как и программные, используют некоторые алгоритмы работы, написанные человеком. А физическая надежность..., аппаратные маршрутизаторы тоже иногда выходят из строя. Кроме того, как я уже сказал, — это дело вкуса. Мне просто нравится работать с программными средствами, которые можно гибко настраивать в зависимости от ситуации, меняющейся очень часто в нашей сети. А надежность защиты — дело рук сисадмина.

— И что, ни разу никаких проблем с защитой?

— Отчего же, были проблемы, когда поставил почтовый сервер, поначалу им стали пользоваться спамеры. Но это продолжалось недолго. Уже на второй день все было сконфигурировано так, как требуется.

— А если сервер рухнет?

— Ну, так что ж, — знаем, где упадем, "подстилаем соломку". Всегда есть резервная копия системы. Храним, как и положено, на отдельном носителе. Восстановление займет не более часа. Железо может, конечно, потребовать несколько большего времени, если выйдет из строя материнская плата, к примеру. Но и выход из строя аппаратных средств потребует времени для замены, если нет уже настроенного резерва.

— Ты не будешь возражать, если я заеду посмотреть на настройки твоего сервера?

— Приезжай, конечно, буду рад тебя видеть! Только посмотри по адресу **http://www.killprog.com/etcr.html** утилиту AntiSpoof v1.1. Она должна помочь тебе защититься от злых хакеров хотя бы на некоторое время.

ГЛАВА 5

Управление рабочими станциями сети

В обязанности администратора сети могут входить и задачи, связанные с администрированием рабочих станций и управлением ими с целью поддержания их в оптимальном состоянии для работы в сети. В этом случае пользователи рабочих станций не вольны делать на них все, что заблагорассудится, а если и сделали что-либо, то при следующей загрузке эти изменения должны быть отменены. Насколько жестким должен быть контроль за конфигурацией рабочих станций, определяется условиями работы администратора сети. В данной главе обсуждаются проблемы обеспечения этого контроля и управления рабочими станциями. Те же средства, что применяются для управления рабочими станциями, могут быть использованы и для управления серверами. Наличие у администратора сети таких средств существенно повышает комфортность и результативность его работы. Возможность удаленного управления и администрирования повышает оперативность устранения проблем, которые могут возникнуть в сети. Применение описываемых в данной главе средств совместно с уже рассмотренными ранее, а также творческий подход к их использованию позволят вам создать уникальный набор инструментов, предназначенных для работы именно в вашей сети.

Установка операционной системы Windows XP в автоматическом режиме

Приобретая рабочие станции для работы в сети, следует придерживаться некоторой стандартизации. В большинстве случаев нет причин чем-либо выделять одну рабочую станцию по сравнению с другой. Приобретать новые компьютеры лучше с предустановленной операционной системой, но может возникнуть потребность самостоятельной установки Windows XP. Устанавливать на новые рабочие станции другую операционную систему в настоящее

время имеет смысл только в исключительных случаях, например, когда программное обеспечение, с которым придется работать пользователю, функционирует только под управлением Windows 98. Но эти случаи теперь достаточно редки.

Повторение установки одной и той же операционной системы в одной и той же конфигурации на нескольких рабочих станциях — занятие мало интересное, отнимающее достаточно много времени и внимания при проведении первоначальных настроек. С целью упрощения этой процедуры и освобождения времени для более интересных дел можно применить средства, предназначенные для автоматизации установки операционной системы.

ОС Windows XP позволяет выполнять автоматическую установку операционной системы с компакт-диска, загрузка с которого должна поддерживаться на компьютере для осуществления автоматической установки системы. Разработчики операционной системы предлагают автоматизировать установку с помощью файла ответов, содержащего все сведения, которые приходится передавать системе в ответ на ее запросы в процессе установки. Для того чтобы подготовить файл ответов, откройте папку Support\Tools, находящуюся на компакт-диске Microsoft Windows XP. В ней находится файл DEPLOY.CAB. Это архив в формате, предложенном Microsoft, который может быть открыт в ОС Windows XP как обычная папка. Создайте на диске своего компьютера папку mensetup (имя можно дать и другое). Скопируйте в нее файл setupmgr.exe, находящийся в DEPLOY.CAB. Это диспетчер установки, с помощью которого может быть создан файл ответов. Запустите диспетчер установки. Создайте файл ответов, следуя инструкциям, появляющимся на экране.

Добавьте в файл ответов раздел [Data] и внесите в него следующие строки:

- `UnattendedInstall=Yes` — указание на необходимость использования файла ответов;
- `MSDosInitiated=No` — указание на необходимость перехода в графический режим после завершения фазы DOS-установки;
- `AutoPartition=1` — указание на необходимость автоматического выбора раздела для установки системы.

Примерный вид созданного файла приведен в листинге 5.1.

Листинг 5.1. Файл Sysprep.inf

```
;SetupMgrTag

[Data]
    UnattendedInstall=Yes
```

```
    MSDosInitiated=No
    AutoPartition=1

[Unattended]
    OemSkipEula=Yes
    InstallFilesPath=C:\sysprep\i386

[GuiUnattended]
    AdminPassword="123456789"
    EncryptedAdminPassword=NO
    OEMSkipRegional=1
    OEMDuplicatorstring="Экспериментальный образ"
    TimeZone=145
    OemSkipWelcome=1

[UserData]
    ProductKey=XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
    FullName="admin"
    OrgName="ap15"
    ComputerName=*

[Display]
    BitsPerPel=16
    Xresolution=800
    YResolution=600
    Vrefresh=60

[TapiLocation]
    CountryCode=7
    Dialing=Pulse
    AreaCode=095

[RegionalSettings]
    LanguageGroup=5,1
    SystemLocale=00000419
    UserLocale=00000409
    InputLocale=00000409

[SetupMgr]
    DistFolder=C:\sysprep\i386
    DistShare=windist

[Identification]
    JoinDomain=ap15.dom
```

```
    DomainAdmin=admin
    DomainAdminPassword=123456789

[Networking]
    InstallDefaultComponents=Yes

[Sysprep]
       BuildMassStorageSection = Yes
[SysprepMassStorage]
```

Измените имя домена, регистрационный ключ, имя и пароль администратора домена и компьютера на нужные вам значения и сохраните полученный файл под именем Winnt.sif на дискете.

Вставьте установочный компакт-диск Windows XP в дисковод для чтения компакт-дисков, а дискету с файлом ответов — в дисковод.

> ***Примечание***
>
> Автоматическая установка должна производиться на единственный раздел. В процессе установки нельзя добавить драйверы независимых производителей.

Если компьютер не загружается, измените порядок загрузки в параметрах CMOS (Complementary Metal-Oxide Semiconductor, энергонезависимая память ПК), чтобы загрузка выполнялась с компакт-диска. Перезагрузите компьютер. Программа установки Windows XP запустится с компакт-диска и использует для автоматической установки файл Winnt.sif, находящийся на дискете.

Этот вариант установки операционной системы позволяет автоматизировать ответы оператора на вопросы системы. Если диск не подготовлен, то придется в самом начале установки согласиться с установкой на выбранный раздел и на его форматирование. Далее все происходит автоматически до самого первого входа в систему. Параметры сети при этом уже настроены. Перед установкой системы на каждый новый компьютер файл ответов следует корректировать в соответствии с новыми параметрами установки. Изменяться могут имя компьютера (если не назначается автоматически), имя администратора компьютера и администратора домена, а также ключ операционной системы.

Для производителей и поставщиков компьютерной техники существует специальный "Пакет предустановки Microsoft Windows XP". Этот пакет позволяет выполнить предустановку операционной системы, что сокращает время ввода в строй нового компьютера. Но применение этого пакета конечными пользователями компьютеров не допускается. Если же вы намерены самостоятельно собирать компьютеры и делать предустановку ОС, то ознакомиться с этой технологией можно на сайте **www.microsoft.com/oem**.

Установка Microsoft Office 2000/XP

Установка офисных приложений, а также изменение их состава в случае неполной установки может отнимать у администратора сети значительное время, особенно когда число рабочих станций достаточно велико. Если вы хотите существенно сократить затраты времени на установку этих программ, доверьте пользователю ввод серийного номера продукта. Дистрибутив следует скопировать на жесткий диск в отдельную папку либо подключить к рабочей станции сетевой диск, на котором он находится. При первом включении компьютера пользователя достаточно перейти в каталог с дистрибутивом и из командной строки запустить программу setup с ключами, которые приведены в следующей строке:

```
setup OEM_ALL=1 ADDLOCAL=ALL /q
```

Установка пройдет в полном объеме без каких-либо вопросов к пользователю.

Даже если вы не хотите доверять процедуру установки офисных приложений пользователю, этот вариант установки сэкономит ваше время: не придется сидеть у компьютера, отвечая на вопросы программы установки.

Установка прочих программных продуктов

Независимо от того, какая программа устанавливается, желательно максимально упростить для пользователя доступ к ее дистрибутиву. Даже рассмотренные выше дистрибутивы операционной системы и MS Office хорошо иметь в каталоге, доступном всем пользователям для чтения. В этом случае любые изменения состава самой ОС, офисных или других программ, применяемых пользователями, не вызовет затруднений, связанных с отсутствием дистрибутивных дисков на своей полке или отсутствием администратора сети на рабочем месте. Наиболее удобно делать первоначальную установку программ из сетевого каталога. Если же в дальнейшем пользователю потребуется изменить состав компонентов программы, ему не придется искать вас и отвлекать от прочих важных дел. Программа сама найдет свой дистрибутив, и пользователю потребуется только указать новый состав компонентов. Иногда при работе с MS Office возникает необходимость в функциях, ранее не требовавшихся. При этом сами офисные программы обнаруживают, что недостает какого-либо компонента, и предлагают установить его. Если дистрибутивы всегда доступны компьютеру пользователя, то ему останется только дать согласие на установку нужного компонента, а все остальное система сделает сама.

Да и самому администратору при установке необходимых программ на компьютеры сети не придется искать дистрибутивы или сетовать на отсутствие

или неисправность дисковода на компьютере пользователя. Во многих случаях вам не придется даже подходить к компьютеру пользователя, достаточно лишь указать ему на место в сети, где расположены необходимые файлы.

Если при создании такой коллекции дистрибутивов придерживаться некоторой системы, располагая в соответствующих папках программы различного назначения, то вы сможете сэкономить довольно много времени на поиске нужных файлов и установке программ на компьютеры пользователей. В состав коллекции дистрибутивов есть смысл включать и коллекцию драйверов устройств, применяемых на рабочих станциях сети.

Клонирование системы, резервный образ

Говоря о клонировании системы (двоичном копировании жестких дисков), следует сразу сказать о необходимости соблюдения лицензионного соглашения с Microsoft. Вы не можете делать копии ОС для установки на другие компьютеры, если не имеете соответствующего числа лицензий. Тем не менее, создать клон системы в качестве эксперимента вам никто не запретит. Нет запрета и на восстановление системы из ее копии на том же компьютере, на котором она уже была установлена, но утрачена в связи с техническими проблемами.

Самый простой путь создания резервного образа диска с системой — это применить программу Acronis True Image, демонстрационную версию которой вместе с информацией о способах приобретения можно найти на странице **http://www.acronis.ru/download/**. Программа может быть запущена как из среды самой операционной системы, так и с загрузочного CD-диска или дискет, созданных средствами самой программы, причем, независимо от способа запуска, она имеет графический интерфейс.

При соблюдении условия идентичности конфигурации компьютеров восстановление системы из образа не вызывает никаких проблем. Удобнее всего создать образ диска с установленной и настроенной системой и сохранить его на загрузочном CD. Если образ не помещается полностью на загрузочном диске, он может быть записан на нескольких носителях. При этом восстановление должно начинаться с последнего диска образа.

С целью оперативности создания резервных образов и их восстановления, для их размещения можно использовать сетевые каталоги. Программа Acronis True Image позволяет, загрузившись с дискет или загрузочного CD, войти в сеть и подключиться к сохраненному образу для его восстановления. Можно определить для себя некую периодичность обновления образа системы, чтобы обеспечить восстановление в случае аварийной ситуации до наиболее актуального состояния. Вероятно, важнее всего иметь резервную ко-

пию системы сервера. Постепенно в процессе эксплуатации сети вами будут добавляться и изменяться различные параметры в ее настройках. Несмотря на ведение журналов и учет всех изменений, восстановление настроек системы после ее краха может потребовать много времени, тогда как восстановление системы из образа диска занимает меньше часа, и при этом все ее настройки уже выполнены. Самое большее, что может потребоваться после завершения процедуры восстановления, это восстановить самые последние данные из архива, периодичность создания которого должна быть не реже одного раза в сутки.

Есть и другие средства для создания резервного образа системы, но корректное создание и восстановление сервера, когда применяются динамические диски для повышения надежности системы, доступно не во всех программах.

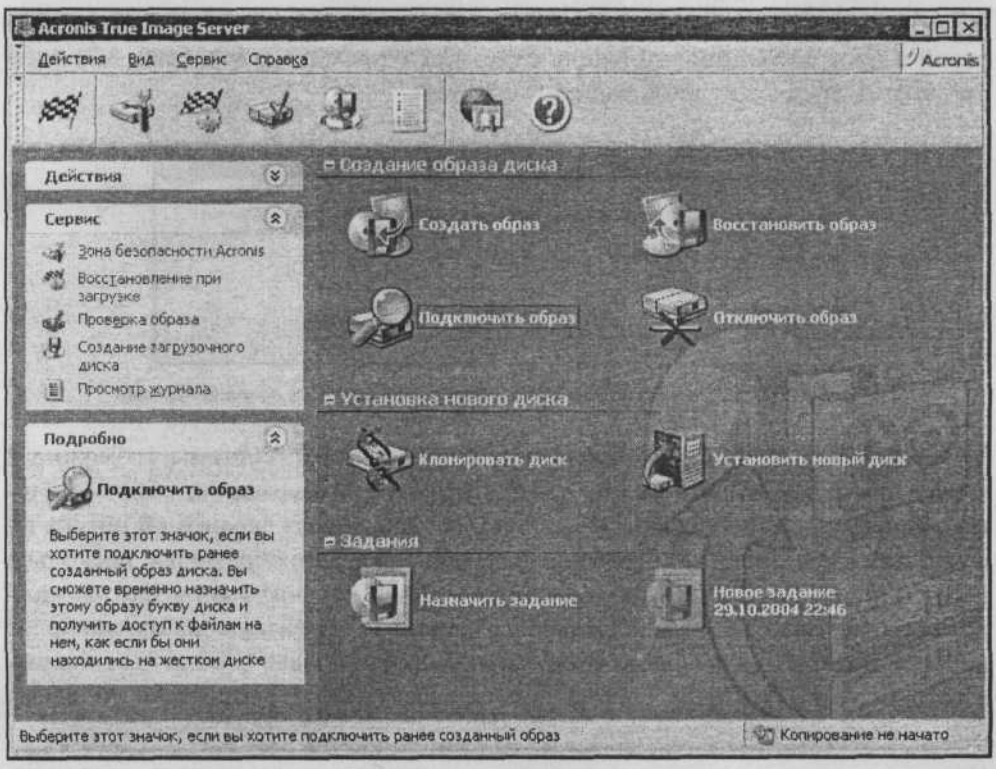

Рис. 5.1. Окно программы Acronis True Image

Программа Acronis True Image (рис. 5.1) позволяет не только создавать образы и восстанавливать их, но и подключать созданный образ в качестве сетевого диска. При этом существует возможность копирования отдельных файлов, содержащихся в образе, если нет необходимости в восстановлении всей

системы. Широкие возможности планирования заданий и их автоматического выполнения позволяют возложить эти функции для основных задач на планировщик программы. В этом случае вы не забудете вовремя дополнить образ актуальными изменениями. Такая автоматизация возможна при установке программы на компьютер, образ системы которого будет создаваться. При запуске процедуры создания образа диска компьютер (сервер, например) может продолжать свою обычную работу. Тем не менее планировать создание и дополнение образа системы лучше на время, когда активность пользователей сети невысока, поскольку процесс создания образа диска несколько замедляет работу системы. Все процедуры работы с дисками и образами осуществляются под управлением программ-мастеров, которые не позволят выполнить некорректную операцию, поставив под угрозу целостность образа или исправность системы.

В случае возможных проблем, возникающих при неправильном выборе действий с программой, пользователь будет предупрежден о них (рис. 5.2) либо программа предложит иной вариант действий.

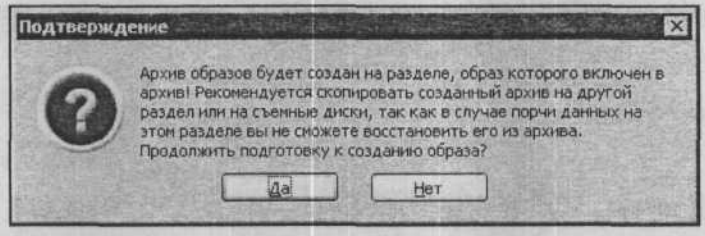

Рис. 5.2. Требование программы подтвердить выбор места создания архива

Учитывая, что полностью корректное восстановление системы возможно в случае идентичности конфигураций компьютера при создании образа системы и в момент его восстановления, следует заботиться заранее об обеспечении этой идентичности. Если для работы в сети приобретается несколько компьютеров, то лучше, чтобы они были одной конфигурации, или, во всяком случае, сходной. Неплохо иметь в запасе материнскую плату наиболее распространенного в вашей сети типа. Весьма полезно, если поставщик, у которого вы приобрели сервер, поддерживает услугу его замены на время ремонта аналогичной моделью.

На самом деле, вы можете не встретиться с проблемами выхода из строя сервера и полной потери данных на нем. И дай Бог! Но, как говорят, "чем черт не шутит...". Все может случиться. Лучше заранее быть готовым к возникновению проблем, чем "кусать локти" и взывать ко всем знакомым о помощи, когда неожиданно "рухнул" сервер.

Удаленное управление

В наше время существует множество средств для удаленного управления и администрирования компьютеров сети. Один из вариантов удаленного управления был рассмотрен в *главе 2*. Средство **Управление компьютером** (которое применяется для управления своим компьютером) может быть подключено и к удаленным машинам для выполнения достаточно широкого круга задач, но далеко не всех. Очень большой круг проблем обслуживания, администрирования и управления рабочими станциями решается только при непосредственном доступе к файловой системе. Тем не менее, если компьютер работает, подключен к сети, а задача состоит в изменении каких-либо параметров системы или выполнении обслуживающих операций, то ваше присутствие около рабочей станции не обязательно. Самая доступная для удаленного управления рабочими станциям сети программа — Telnet. Telnet-клиент существует во всех операционных системах Windows. Сервер Telnet встроен только в системы, начиная с Windows 2000 и старше. Если в вашей сети на рабочих станциях установлена ОС Windows XP, то все они имеют в своем составе сервер Telnet. Для запуска этого сервера на рабочих станциях сети можно воспользоваться средством **Управление компьютером** или **Службы** (Services) из папки **Администрирование**.

Подключившись к требуемому компьютеру (рис. 5.3), запустите на нем службу Telnet.

Если на каждой рабочей станции запущен сервер Telnet, вы можете на них выполнять практически все операции, доступные из командной строки: подключать и отключать сетевые диски, копировать файлы, запускать на выполнение программы и командные файлы. К сожалению, этим способом невозможно установить сложные пакеты программ, подобные Microsoft Office, но для установки простых программ, не требующих сложных процедур регистрации, а также для проведения операций с файлами и папками это средство вполне подходит. Возможно, что для нормальной работы с Telnet-сервером на рабочих станциях, работающих под управлением Windows 2000/XP Professional, первичную настройку придется производить непосредственно на них. Чтобы запустить эту службу, воспользуйтесь следующей командой из командной строки:

```
net start telnet
```

Если нужно, чтобы сервер стартовал автоматически при запуске системы, следует изменить режим запуска с ручного на автоматический.

По умолчанию сервер пытается аутентифицировать клиента по схеме NT LAN Manager (NTLM), что позволяет регистрироваться автоматически, если подключение происходит с компьютера, где вы уже зарегистрированы в ка-

честве администратора домена. Для удаленного доступа из-за пределов локальной сети это неудобно; чтобы сменить режим аутентификации, сначала нужно запустить из командной строки утилиту администрирования сервера Telnet командой:

```
Tlntadmn config sec = -NTLM +passwd
```

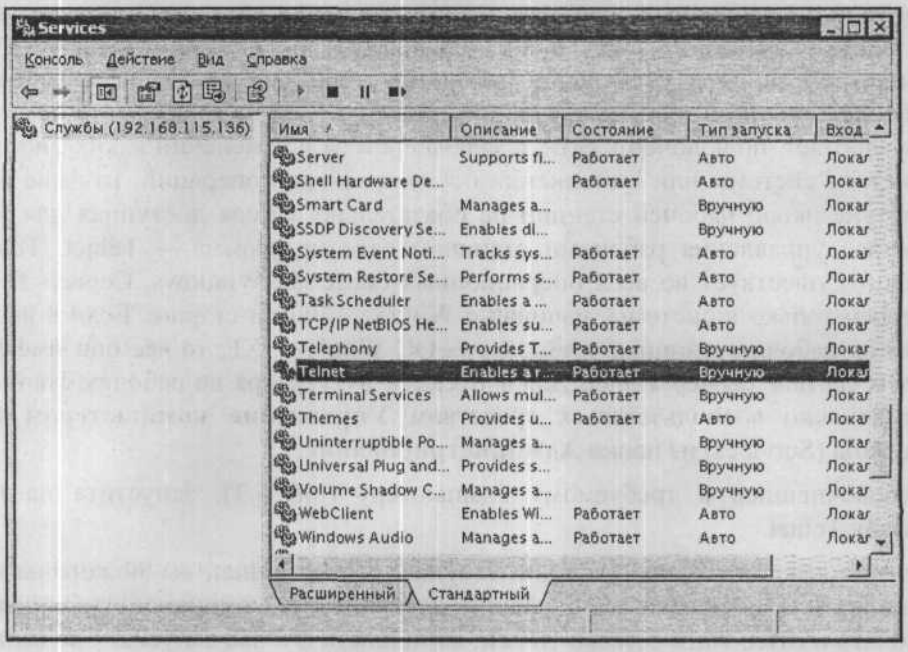

Рис. 5.3. Служба Telnet на удаленном компьютере

После установки параметров аутентификации вы сможете управлять рабочими станциями из любой точки сети и даже через Интернет, авторизовавшись в качестве администратора этой рабочей станции. Если доступ к рабочим станциям осуществляется только из локальной сети, то режим аутентификации следует установить следующей командой:

```
Tlntadmn config sec = +NTLM +passwd
```

Получив доступ к рабочей станции, вы можете выполнить на ней все программы, которые не используют графический интерфейс.

Примечание

Следует иметь в виду, что по протоколу Telnet пароль передается в открытом виде. Это средство управления компьютерами через Интернет следует применять, если вы уверены, что никто не перехватит пароль во время авторизации, а сам пароль достаточно сложен, что исключит возможность его подбора.

Задачи, доступные через Telnet

Defrag

Каждая рабочая станция сети требует периодического обслуживания. Одна из периодически выполняемых операций — дефрагментация дисков. Через Telnet доступна команда Defrag. Вызываемая этой командой программа не имеет графического интерфейса, все отчеты выводятся в текстовом виде на экран или в файл. Команда может выполняться в фоновом режиме. Это значит, что пользователь будет продолжать работу, не подозревая, что в это время проводится обслуживание его рабочей станции.

`Defrag c:\ /a` — выводит отчет об анализе тома C:\ на необходимость проведения дефрагментации.

Schtasks

Команда позволяет создать задание подобно тому, как это делается в планировщике заданий Windows. Полный перечень возможностей команды лучше посмотреть в справке по ней. Ознакомившись со справкой, вы увидите ее полезность для администрирования компьютеров.

Более старый аналог этой команды — **At**.

Chcp

В ряде случаев, мы можем встретиться с ситуациями, когда на экран сеанса Telnet или просто командной строки выводятся "кракозябры". Для согласования кодовой страницы, в которой осуществляется вывод информации, с кодовой страницей самого окна сеанса работы, и может быть использована эта команда со следующими параметрами:

- `Chcp 866` — включаем вывод в кодировке DOS;
- `Chcp 1251` — вывод в кодировке Windows;
- `Chcp` (без параметров) — показать текущую кодовую страницу.

Интересно, что даже встроенные в Windows программы командной строки не всегда корректно выводят свои сообщения, особенно при удаленном доступе к компьютеру. Подправив вывод символов на экран, получим возможность комфортной работы с такими программами. Иногда есть необходимость выполнить целую серию команд, результат которых выводится в разных кодировках. Для ускорения работы в подобных случаях лучше выполнять команды с перенаправлением вывода в текстовый файл. Затем следует скопировать этот файл на свой компьютер и читать его с помощью файлового менеджера FAR. В этом файловом менеджере переключение кодировки при чтении файла выполняется нажатием кнопки <F8>.

Ipconfig

Как и при работе на локальной машине, данная команда позволяет просмотреть и обновить конфигурацию IP-протокола. В режиме удаленного доступа команда будет доступна, если компьютер исправен и IP-протокол функционирует верно. Поэтому применение этой команды на удаленных рабочих станциях в основном ограничено получением сведений о конфигурации путем ввода команды:

```
ipconfig /all
```

Openfiles

Команда позволяет увидеть перечень открытых сетевыми пользователями общих файлов.

Используемые параметры:

- `openfiles.exe /query` — основной вариант выполнения команды;
- `openfiles.exe /query /fo table /nh` — вывод информации в виде таблицы без заголовка;
- `openfiles.exe /query /s srvmain /u maindom\hiropln /p p@ssW23` — вывод информации об открытых файлах на другом компьютере сети. В моей практике команда применяется, когда я подключаюсь из дома к серверу, доступному из Интернета, а затем определяю список открытых файлов на другом сервере или компьютере сети.

При использовании Telnet для связи с сетью из Интернета пароли и имена пользователей передаются в открытом виде. Поэтому применять этот протокол лучше уже внутри сети, а из Интернета использовать данный вариант связи с сетью только в исключительных случаях и ограниченно.

Организация подключения к серверу сети из Интернета может быть реализована с применением возможностей сервера терминалов или удаленного доступа к рабочему столу.

Удаленный доступ к рабочему столу

ОС Windows XP имеет в своем составе программу **Подключение к удаленному рабочему столу** (рис. 5.4).

Эта программа позволяет устанавливать связь как с удаленными рабочими столами, так и с серверами терминалов, для которых ранее требовалась установка клиента сервера терминалов. Серверные операционные системы содержат в своем составе компоненты сервера терминалов и по умолчанию допускают два подключения для администраторов, не требующие дополни-

тельного лицензирования. Настроив подключение к серверу с удаленной машины, можно сохранить параметры подключения в виде файла с расширением rdp, в котором они будут записаны в виде обычного текста. Сохранив несколько таких файлов, можно оперативно подключаться к требуемым компьютерам.

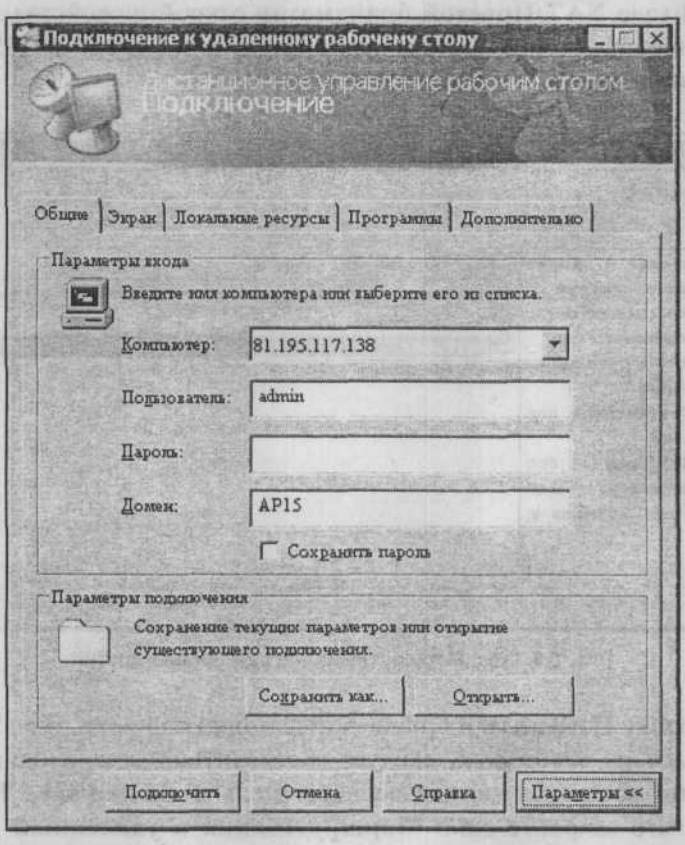

Рис. 5.4. Окно программы **Подключение к удаленному рабочему столу**

Не возникает трудностей и при подключении к серверам или рабочим станциям с помощью этого средства изнутри сети. Определенные проблемы могут возникнуть, когда вы решите организовать доступ с помощью этой программы к серверу сети из Интернета. Поскольку подключенный к Интернету сервер должен быть защищен от проникновения непрошеных гостей, на нем запущен брандмауэр, не допускающий прохождение в сеть пакетов, не запрошенных из нее. Настраивая маршрутизацию пакетов в сеть, можно для порта TCP 3389 указать любой адрес внутри сети в качестве получателя внешних пакетов. При этом, указывая внешний адрес сервера, подключенно-

го к Интернету, при условии правильного ввода пароля, имени пользователя и домена, вы получите подключение к компьютеру или серверу, находящемуся внутри сети.

В качестве примера приведем вариант настроек, примененный в нашей сети.

Откройте **Администрирование | Маршрутизация и удаленный доступ** (рис. 5.5). В узле **NAT/Простой брандмауэр** откройте свойства интерфейса, подключенного к Интернету. На вкладке **Службы и порты** (рис. 5.6) найдите **Дистанционное управление рабочим столом**.

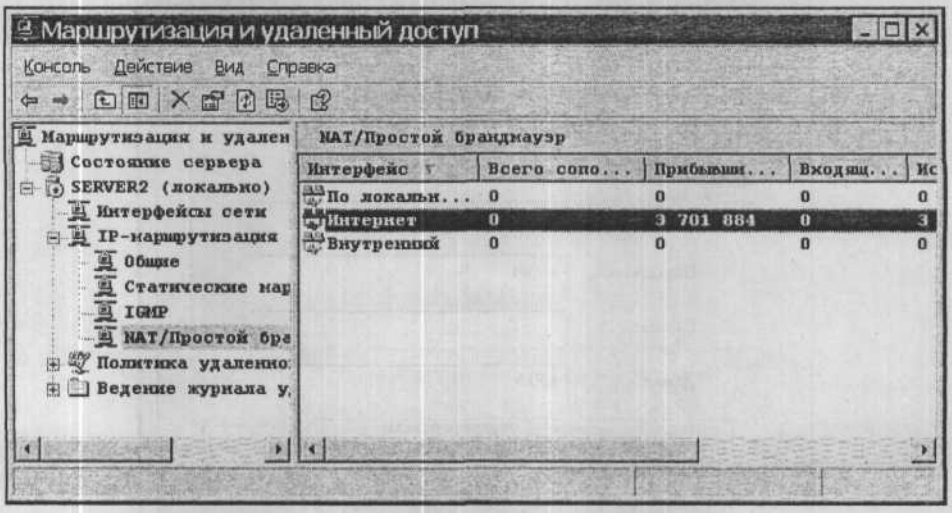

Рис. 5.5. Окно **Маршрутизация и удаленный доступ**

Нажмите кнопку **Изменить** и в поле **Адрес в частной сети** (рис. 5.7) введите адрес компьютера, к которому следует обеспечить подключение из Интернета. Сохраните настройки, нажав последовательно кнопки **OK**, **Применить**, **OK**, после чего закройте окно **Маршрутизация и удаленный доступ**. Теперь, подключаясь из Интернета, вы попадете не на сервер, через который осуществляется подключение, а на указанный вами компьютер.

Учитывая, что передача пароля и имени пользователя производится в зашифрованном виде, этот вариант связи с сетью из Интернета более предпочтителен, чем Telnet. Но, установив связь с любым компьютером или сервером сети через удаленный рабочий стол, вы можете использовать все возможности Telnet для управления другими компьютерами этой сети (рис. 5.8).

Во время сеансов связи через удаленный рабочий стол или сервер терминалов следует учитывать, что после установления связи сеанс будет открыт, даже если вы закроете окно сеанса у себя на компьютере, или физически прервется

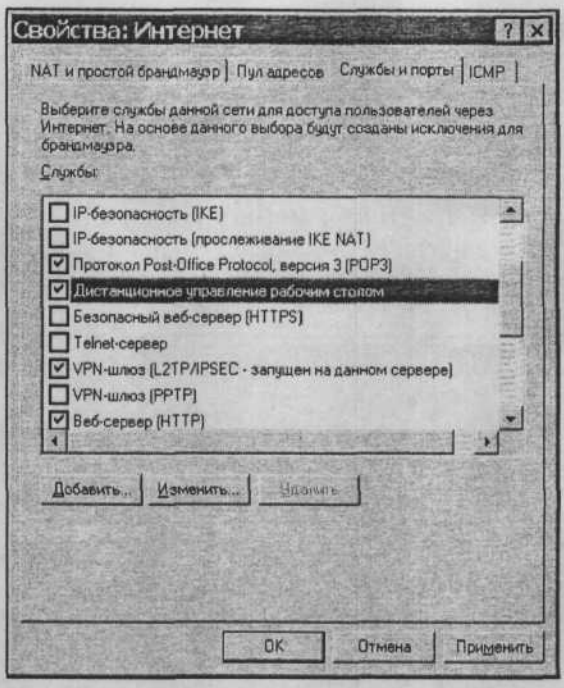

Рис. 5.6. Свойства интерфейса **Интернет**, вкладка **Службы и порты**

Рис. 5.7. Окно **Изменить службу**

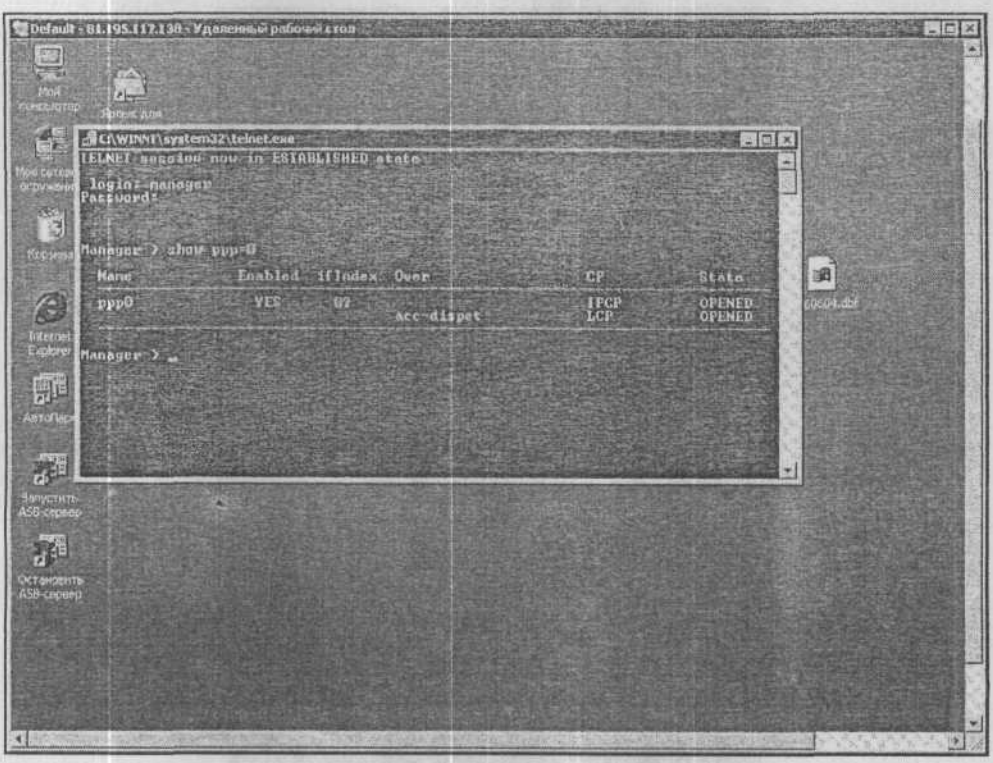

Рис. 5.8. Сеанс связи с одним из серверов сети через Интернет

связь. Если вы не установите ограничение на время бездействия во время сеанса, то после двух попыток связи вы исчерпаете лимит на количество сеансов администраторов. Обязательно корректно завершайте сеансы работы!

Следует иметь в виду, что подключение к рабочему столу обычной рабочей станции приведет к закрытию сеанса пользователя. Более того, если рабочая станция зарегистрирована в домене, сеанс будет блокирован, и только администратор компьютера сможет снять блокировку. В нашей сети есть необходимость для отдельных пользователей подключаться к рабочему столу одной из рабочих станций для доступа к программе, которая не может быть установлена на других компьютерах. Чтобы обеспечить возможность такого подключения без блокировки сеанса (только закрытие с сохранением работы всех программ), эту рабочую станцию пришлось вывести из состава домена, она работает в своей отдельной рабочей группе. Иногда это создает неудобства при подключении к компьютерам и серверам сети, поскольку они не отображаются в сетевом окружении этой рабочей станции. Тем не менее, найдя компьютер по IP-адресу, можно подключиться к его доступным ресурсам, введя имя пользователя домена и пароль.

Radmin

Как альтернативный вариант подключения к серверу сети из Интернета, можно применить и программу удаленного администрирования Radmin (Remote Administrator) (рис. 5.9).

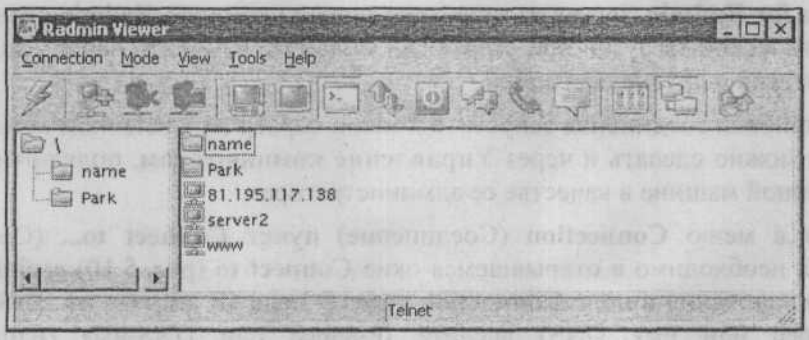

Рис. 5.9. Окно Radmin Viewer

Эта программа дистанционного управления и администрирования, которая позволяет вам работать на удаленном компьютере с вашего рабочего места. При этом вы видите экран удаленного компьютера на своем рабочем столе в окне или развернутым на весь экран, а ваша мышь и клавиатура подменяют мышь и клавиатуру на удаленном компьютере, если управление осуществляется в полноэкранном режиме или окно удаленного экрана активно. В отличие от программы дистанционного управления рабочим столом, Radmin не позволяет работать с видеопроигрывателями на удаленном компьютере, получать с их помощью звуки. Эта программа предназначена только для администрирования удаленных рабочих станций.

Программа имеет несколько режимов работы:

- Режим полного контроля
- Режим просмотра
- Режим командной строки (Telnet)
- Режим обмена файлами

Кроме того, в последней версии Radmin Viewer предусмотрены режимы, поддержка которых должна появиться в ближайшее время и в серверной части программы, устанавливаемой на компьютере, с которым осуществляется связь. Это режимы текстового и голосового чата, а также отправка коротких текстовых сообщений. Они предназначены для удаленной работы с пользователем или помощником администратора.

Текущая версия серверной части программы не поддерживает эти дополнительные функции, но для индивидуальной удаленной работы они и не требуются.

После установки программы вы можете стартовать ее серверную или клиентскую часть из меню **Пуск** (Start). Также возможен запуск настройки сервера **Settings for Radmin Server** из меню, где можно настроить Radmin-сервер для автоматической загрузки при старте ОС Windows, изменить пароль для сетевого доступа и другие настройки.

Для установки соединения запустите Radmin-сервер на удаленном компьютере. Это можно сделать и через **Управление компьютером**, подключившись к удаленной машине в качестве ее администратора.

Выбрав в меню **Connection** (Соединение) пункт **Connect to...** (Соединение с...), необходимо в открывшемся окне **Connect to** (рис. 5.10) выбрать режим подключения в поле **Connection type**. В поле **IP address or DNS name** (IP адрес или имя DNS) введите IP-адрес или DNS-имя (например: comp1.company.com) удаленного компьютера, на котором запущен Radmin-сервер.

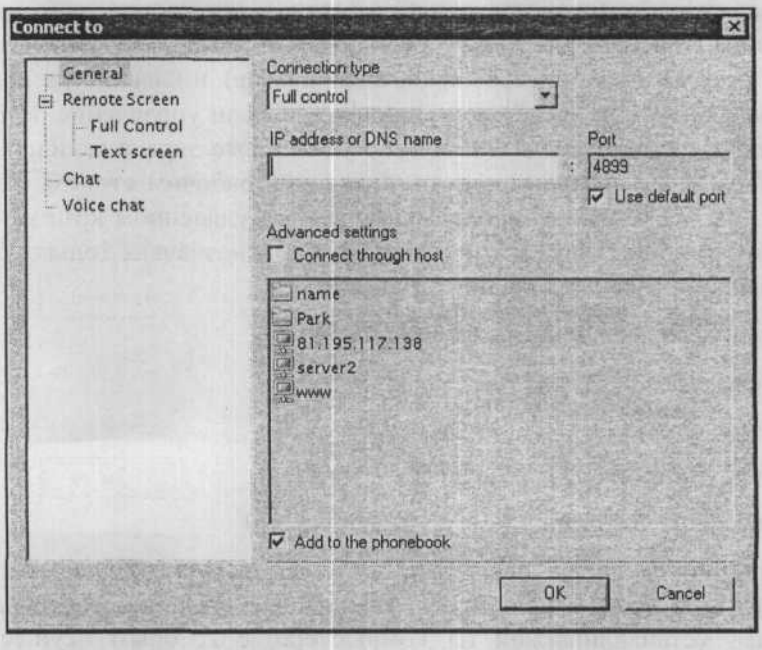

Рис. 5.10. Окно **Connect to** (выбор режима работы и адреса для подключения)

Если при установке программы не изменялся номер порта и этот номер не запрещен маршрутизатором или брандмауэром, то установится соединение.

В зависимости от настроек серверной части программы, может потребоваться ввод пароля для подключения или ввод имени пользователя, пароля и имени домена. Созданное соединение может быть сохранено для оперативного подключения в следующий раз.

Для обеспечения возможности работы с компьютерами всей сети через один компьютер (удобно, когда прямое подключение возможно только к одному компьютеру) существует режим **Connect trough host** (подключение через компьютер). Этот режим позволяет физически подключиться к компьютеру, доступному из Интернета, например, а уже через него — к любому компьютеру сети, где работает Radmin-сервер.

Подключаясь через Интернет, важно заранее знать IP-адрес удаленного компьютера или иметь возможность определить его. Поскольку в нашей сети есть постоянное подключение к Интернету, IP-адрес сервера с внешней стороны постоянный. В других случаях можно использовать средства администрирования по электронной почте. Отправив служебное сообщение, содержащее соответствующую команду (сценарий), можно в ответе получить IP-адреса необходимых компьютеров.

Настройка Radmin-сервера

Для успешной работы с новыми операционными системами требуется версия 2.2 программы Remote Administrator (Radmin).

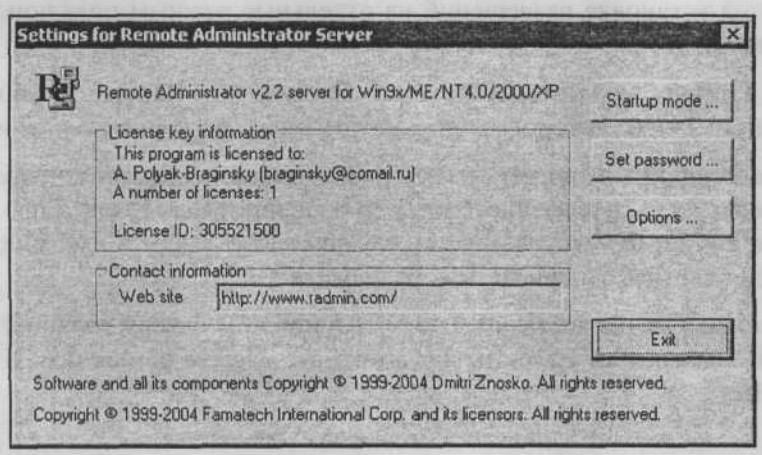

Рис. 5.11. Окно **Settings for Remote Administrator Server** (Настройка **Remote Administrator Server**)

Выбрав в меню **Пуск | Программы | Remote Administrator | Settings for Remote Administrator Server**, вы откроете окно (рис. 5.11), из которого можно получить доступ к различным настройкам Radmin-сервера. Кнопкой

Startup mode вызывается окно выбора варианта запуска сервера: можно выбрать ручной или автоматический запуск. Опция **Set password** позволяет установить пароль для подключения к серверу (рис. 5.12).

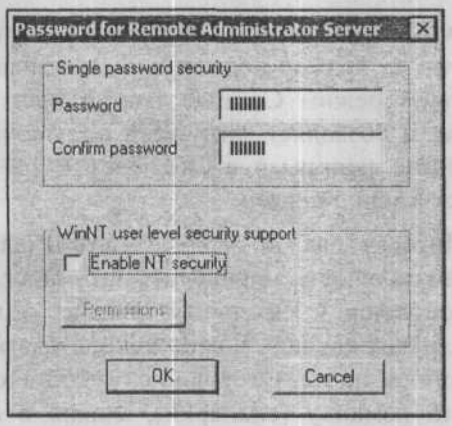

Рис. 5.12. Окно **Pasword for Remote Administrator Server** (Пароль для **Remote Administrator Server**)

Включив в этом окне опцию **Enable NT security**, вы сможете установить разрешение для доступа на уровне системы NTFS, выбрав необходимых пользователей и разрешения для них (рис. 5.13).

Допускается установка разрешений на отдельные режимы подключения или на все сразу.

Кнопкой **Options** можно вызвать окно **Options for Remote Administrator Server** (рис. 5.14), из которого доступно несколько дополнительных настроек.

В разделе **Logging** можно установить режим записи событий подключения к Radmin-серверу в журнал системных сообщений (**Use Event Log**) и/или в файл (**Use logfile**). В текстовом поле можно указать адрес и имя файла, в который будет вестись запись протокола событий.

Есть возможность предоставлять доступ к Radmin-серверу только с определенного IP-адреса или подсети, для этого вы можете установить IP-фильтр (**Use IP filter**).

Пример

Для доступа из целой подсети установите:

Фильтр IP (**IP filter**) — 192.168.115.0

Маска (**Subnet mask**) — 255.255.255.0

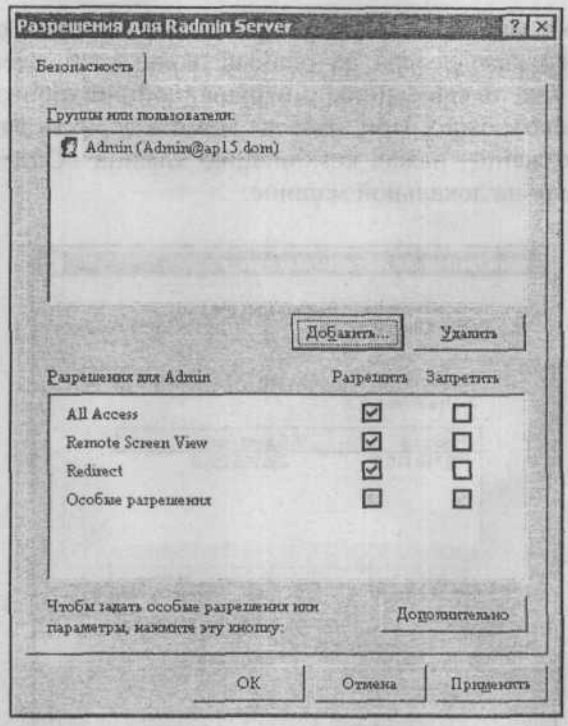

Рис. 5.13. Окно **Разрешения для Radmin Server**

Для доступа с определенного компьютера установите:

Фильтр IP (**IP filter**) — 192.168.115.90

Маска (**Subnet mask**) — 255.255.255.255

Естественно, что необходимо вводить свои адреса.

Программа Radmin использует по умолчанию порт 4899, но при желании вы можете изменить это значение на любое, не используемое другими приложениями и службами. Для этого используйте раздел **Port** (см. рис. 5.14).

В разделе **Incoming connection dialog** (диалог при подключении) можно установить необходимость разрешения пользователя на подключение и действия программы при отсутствии разрешения. Программа может через установленное время отклонить доступ или разрешить его, несмотря на отсутствие такого разрешения.

Программа Radmin не регистрирует экранные изменения, если удаленный компьютер находится в полноэкранном текстовом режиме. В таком режиме GDI (Graphic Device Interface, интерфейс графических устройств) не выполняет прорисовку экрана. Работа в текстовом режиме на удаленной машине

возможна только в оконном режиме. При разворачивании окна командной строки удаленного компьютера на полный экран изображение удаленного экрана выглядит как телевизионное с нарушенной синхронизацией, поэтому работать с ним невозможно. При этом вы можете вернуть оконный режим и устойчивое изображение, нажав комбинацию клавиш <Ctrl>+<Enter>, как и при обычной работе на локальной машине.

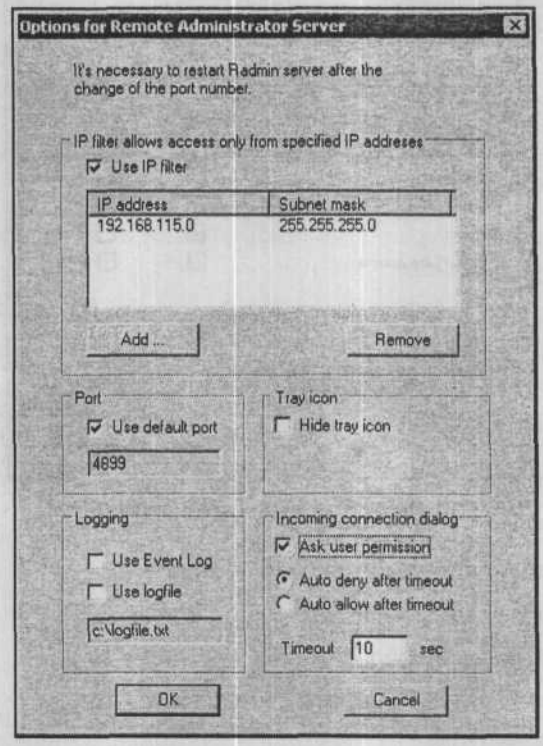

Рис. 5.14. Окно **Options for Remote Administrator Server** (Опции **Remote Administrator Server**)

Как клиентская, так и серверная части программы могут гибко управляться из командной строки.

Для управления клиентской частью используются следующие ключи:

- radmin.exe /connect:xxxxx:nnnn — указывает сервер и порт для подключения;
- radmin.exe /connect:xxxxx:nnnn /through:xxxxx:nnnn — указывает адрес и порт промежуточного сервера.

По умолчанию устанавливается режим соединения **Full Control** (Полный контроль), позволяющий видеть удаленный экран, управлять мышью и клавиатурой).

Для установки других режимов соединения используются следующие команды:

- radmin.exe /connect:xxxxx:nnnn /noinput — режим просмотра (видишь только экран);
- radmin.exe /connect:xxxxx:nnnn /shutdown — режим удаленного выключения компьютера;
- radmin.exe /connect:xxxxx:nnnn /file — режим пересылки файлов;
- radmin.exe /connect:xxxxx:nnnn /telnet — Telnet-режим.

Следующие далее настройки работают только в режимах **Full Control** (Полный контроль) и **View** (Просмотр):

- radmin.exe /connect:xxxxx:nnnn /fullscreen — устанавливает полноэкранный режим просмотра;
- radmin.exe /connect:xxxxx:nnnn /hicolor — устанавливает формат цвета для передачи по сети, равный 65 536 цветам;
- radmin.exe /connect:xxxxx:nnnn /locolor — устанавливает формат цвета для передачи по сети, равный 16 цветам;
- radmin.exe /connect:xxxxx:nnnn /updates:nn — указывает максимальное количество прорисовок для просмотра;
- radmin.exe /connect:xxxxx:nnnn /encrypt — включает шифрование всех данных при работе.

Возможны другие настройки:

- radmin.exe /connect:xxxxx:nnnn /unregister — удаляет все уже введенные ключи для Radmin;
- radmin.exe /? — показывает окно помощи.

Управление серверной частью осуществляется с помощью следующих команд:

- r_server.exe /setup — показывает диалог (запускает мастера), который вам поможет установить сервис и драйвер, а также указать пароль и номер порта для Radmin-сервера;
- r_server.exe /setup /port:xxxx, r_server.exe /setup /pass:xxxxx — если не имеется никаких других определенных переключателей, за исключением /port and /pass, r_server выполняет как Radmin-сервер;
- r_server.exe /setup /save [/port:xxxx] [/pass:xxxxx] — позволяет изменить номер порта и/или пароль в реестре;
- r_server.exe /setup /install — установка как сервиса (службы);
- r_server.exe /setup /uninstall — деинсталляция программы Radmin-сервер;

- r_server.exe /setup /installservice — установка только сервиса (т. е. программа просмотра не устанавливается совсем, а Radmin-сервер устанавливается как служба;
- r_server.exe /setup /silence — не показывать сообщения "error" или "ok" в командах /install, /uninstall или /save;
- r_server.exe /stop — останавливает Radmin-сервер. Эта команда останавливает сервис и завершает приложение. Для остановки сервиса под WinNT требуется наличие соответствующих прав.

  Для остановки сервера можно использовать соответствующий ярлык в папке Remote Administrator.

Большой набор команд для работы из командной строки позволяет выполнить множество операций по настройке Radmin на удаленном компьютере, воспользовавшись уже настроенным Telnet-подключением.

Применение программы Radmin возможно и на компьютерах с ОС Windows 98.

Сетевой профиль

Редко кто из сетевых администраторов применяет это свойство учетной записи. Но если вы хотите максимально унифицировать рабочие станции и их настройки, следует использовать сетевые профили.

Применение сетевого профиля позволяет сохранять рабочий стол в неизменном виде при каждом входе пользователя в сеть. Добавление к профилю HTML-страницы, внедренной в рабочий стол, позволит передавать пользователям необходимую информацию в текстовом и графическом виде, а также ссылки на файлы, расположенные в сети, для обеспечения их загрузки или выполнения. Конечно, "продвинутые" пользователи могут попытаться изменить эти настройки и отменить загрузку обязательного профиля. Для исключения такой возможности следует сохранять пароль администратора компьютера, созданный при установке системы, в секрете, а также не давать рядовым пользователям прав администратора рабочей станции. Кроме того, регулярное создание архивной копии системы позволит оперативно восстановить настройки рабочей станции при их преднамеренном или случайном нарушении.

Подключить сетевой профиль нетрудно. В свойствах каждого пользователя сети есть возможность указать путь к сетевому профилю. Если применяются локальные учетные записи (в отдельных случаях без этого не обойтись), следует указать тип профиля и путь к нему в процессе настройки рабочих станций.

Профили можно заранее заготовить для различных категорий пользователей. Сетевые пользователи получат дополнительное преимущество, независимо от того, с какой рабочей станции они входят в сеть, вид рабочего стола и ярлыки к программам будут неизменны. Пользователи в любой момент могут закрыть лишние элементы рабочего стола, но при следующей загрузке компьютера эти элементы появятся вновь.

По ссылкам на HTML-страницах, внедренных в рабочий стол (рис. 5.15), могут запускаться как программы, так и сценарии установки программ, либо — загружаться файлы, возможность и необходимость загрузки которых определена вами на данный момент.

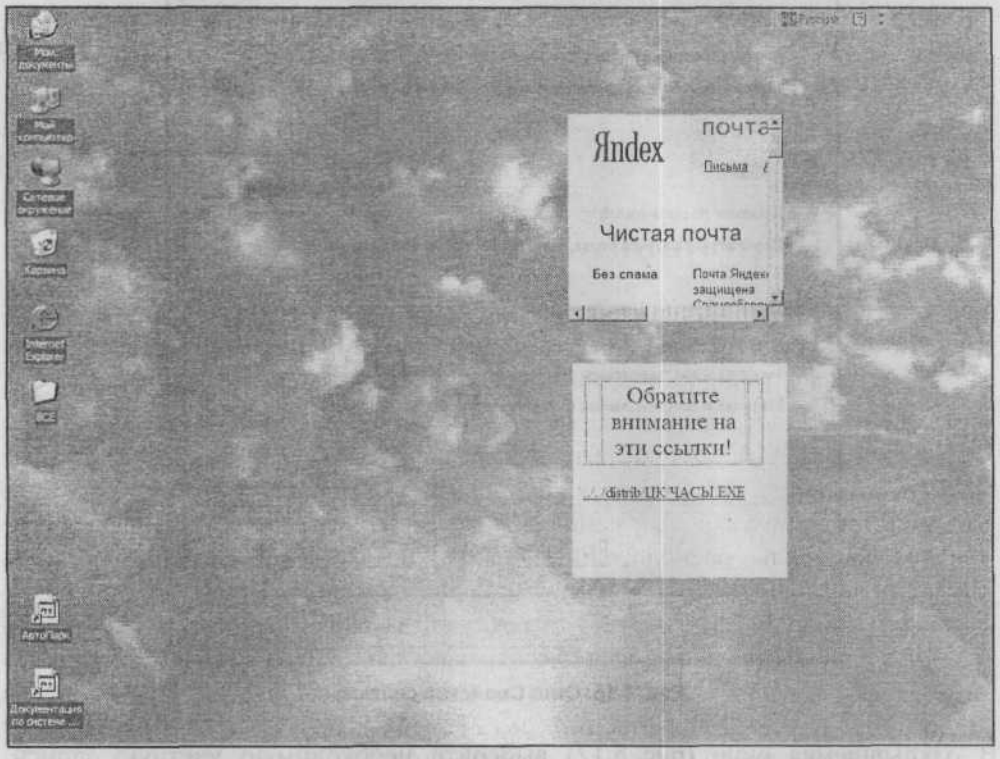

Рис. 5.15. Рабочий стол сетевого профиля с внедренными HTML-страницами

Профили локальных пользователей компьютера должны сохраняться в локальном каталоге, а профили сетевых пользователей, которых должно быть большинство, следует сохранять на сервере, иначе при входе в сеть с разных компьютеров профиль не удастся загрузить.

Для настройки профиля необходимо выполнить определенную последовательность действий.

Войдите в систему под учетной записью администратора компьютера и домена.

Затем откройте **Панель управления | система** (рис. 5.16), вкладку **Дополнительно** в окне **Свойства системы**. В разделе **Профили пользователей** нажмите кнопку **Параметры**.

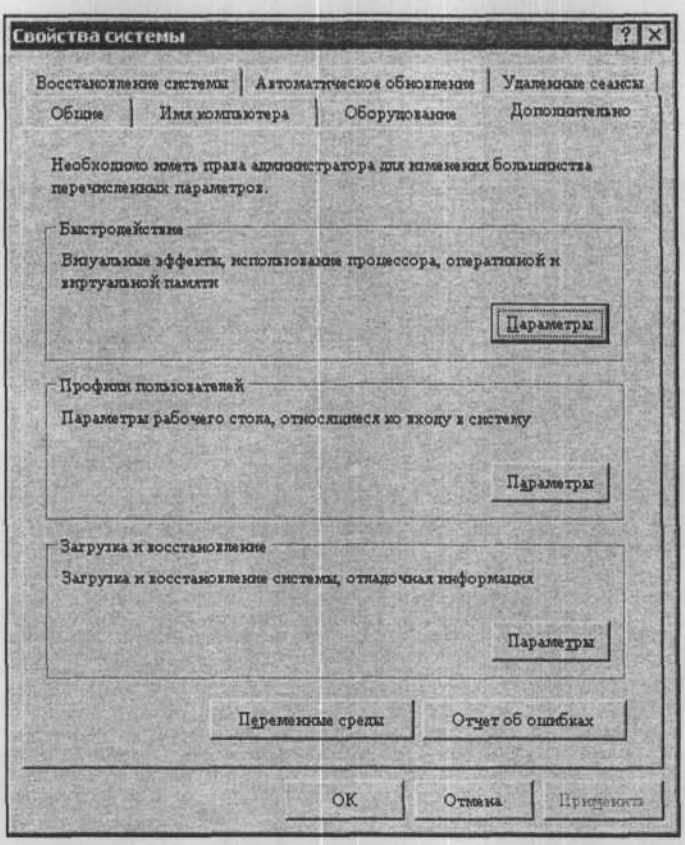

Рис. 5.16. Окно **Свойства системы**

В открывшемся окне (рис. 5.17) выберите необходимую учетную запись пользователя и нажмите кнопку **Сменить тип**.

Если переключатель **Перемещаемый профиль** не доступен, как на рис. 5.18, то следует создать перемещаемый профиль на сервере.

Для этого можно поступить следующим образом. Сначала в свойствах учетной записи в **Active Directory Users and Computers** на сервере укажите путь к профилю (рис. 5.19). Путь можно указать к любому каталогу на любом компьютере или сервере, где вы решили сохранять профили пользователей.

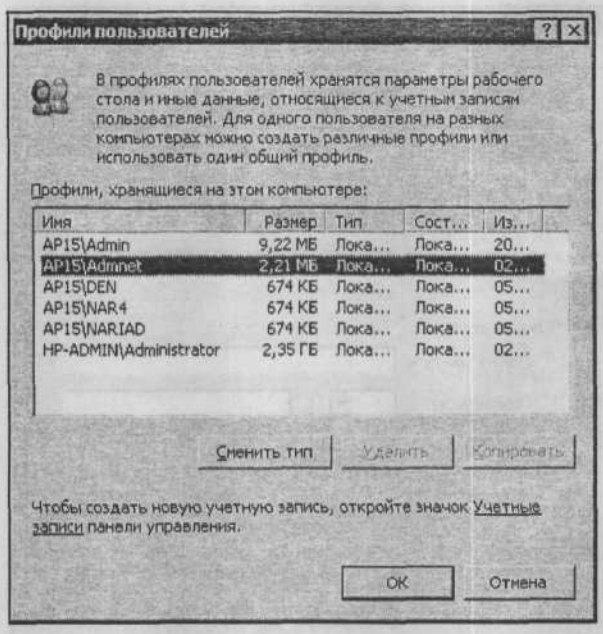

Рис. 5.17. Окно **Профили пользователей**

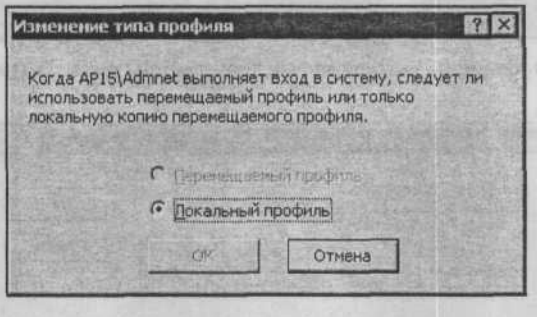

Рис. 5.18. Изменение профиля пользователя

Настройте параметры рабочего стола компьютера так, как необходимо для работы этого пользователя.

Откройте окно **Профили пользователей** на локальном компьютере, выделите учетную запись и нажмите кнопку **Копировать** (рис. 5.17).

В открывшемся окне **Копирование профиля** (рис. 5.20) укажите путь для копирования и нажмите **OK**.

После этого, нажав кнопку **Изменить** (рис. 5.20), найдите учетную запись пользователя для разрешения использовать профиль.

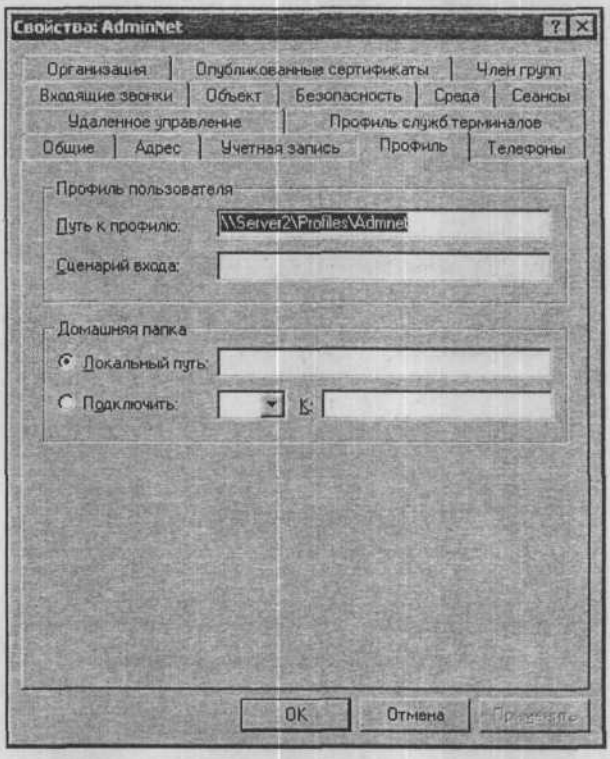

Рис. 5.19. Свойства учетной записи пользователя (вкладка **Профиль**)

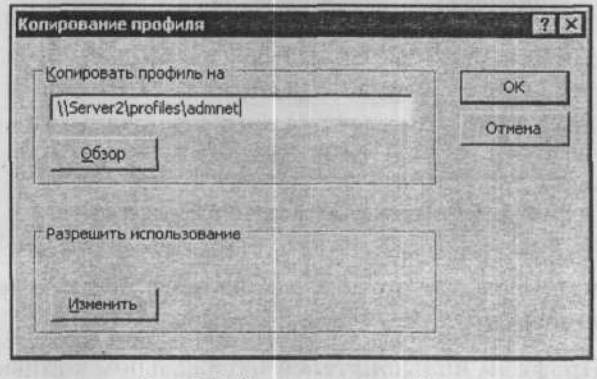

Рис. 5.20. Копирование профиля

Через одну-две минуты зарегистрируйтесь в системе с учетной записью пользователя и убедитесь, что его профиль стал перемещаемым (рис. 5.21).

Теперь вы можете дать разрешение на использование этого профиля и другим пользователям, если их профиль должен быть таким же. Можно поместить

всех пользователей, которые будут применять этот профиль, в специальную группу, которой дать соответствующее разрешение. Если не указывать конкретные разрешения на использование профиля, то профиль будет необязательным. Для того чтобы пользователь не мог изменить профиль и его тип, следует в папке его профиля на сервере изменить имя файла NTUSER.DAT на NTUSER.MAN. В этом случае станет недоступной опция **Локальный профиль** в его настройках для этого пользователя.

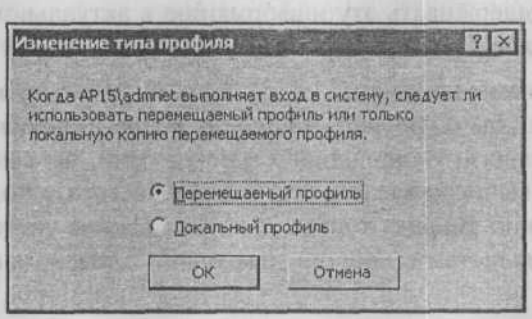

Рис. 5.21. Окно **Изменение типа профиля** (опция **Перемещаемый профиль**)

Применив перемещаемые профили, вы получите некоторые дополнительные возможности, например, сможете помещать в папку **Desktop** (Рабочий стол), находящуюся в папке профиля, файлы, которые пользователь увидит на своем рабочем столе при входе в систему. Все это позволяет передавать важную информацию для всех пользователей профиля.

При использовании перемещаемого профиля несколькими пользователями, папка **Мои документы** оказывается общей для всех этих пользователей, точнее, при входе в систему загружается папка со всеми изменениями, сделанными другими пользователями профиля. Есть возможность задать для каждого пользователя отдельную папку при настройке профиля пользователя (см. рис. 5.19), указав имя и адрес в поле **Домашняя папка**. При этом можно указать как локальную, так и сетевую папку. Второй вариант предпочтительнее, если пользователь имеет обыкновение входить в сеть с разных рабочих станций.

Можно указать и адрес сценария, который будет выполняться при входе в систему и подключать, например, необходимые для работы сетевые диски. В качестве файла сценария допускается применять как обычный пакетный файл, так и файлы сценариев.

При таких настройках пользователь оказывается практически независимым от рабочей станции. Откуда бы он ни вошел в сеть, он всегда будет работать в привычной среде со своими документами.

Учет рабочих станций

Установить должный порядок в учете оборудования и установлении четкого графика обслуживания вычислительной техники в сети мешает либо отсутствие необходимых кадров, либо лень администратора, либо другие причины. Если для вас эта проблема актуальна, то можно обратиться к бесплатной программе, которая поможет собрать очень подробные сведения обо всех компьютерах сети, поддерживать эту информацию в актуальном состоянии, вести плановое обслуживание и учет ремонтов вычислительной техники сети.

Есть у этой программы некоторые недостатки: будучи запущенной из сетевого каталога, она как бы подвисает, но вполне корректно работает при запуске из локального каталога. Освоившись с программой, вы сможете сформировать базу данных вычислительной техники своей сети с подробностями, которые обычно можно собрать только при тщательном учете поступающей к вам техники специалистами, хорошо знакомыми с информационными технологиями.

Программа позволяет получать отчеты, форму которых можно корректировать самостоятельно, учитывать сведения о ремонтах и модернизациях. Найти это средство учета компьютеров можно по адресу: **http://checkcfg.narod.ru/**.

Строго говоря, это не одна программа, а комплект программ, состав которого может быть изменен в определенных пределах по вашему усмотрению. В качестве основных компонентов комплекта необходимо использовать два — sklad и checkcfg. Первый из них (рис. 5.22) и есть собственно программа учета оргтехники (не только компьютеров), а второй — программа для сбора сведений о компьютерах. Другие компоненты, например Doberman, который позволяет отследить изменения в конфигурации компьютеров с момента последнего сбора данных, не обязательны. Компонент sklad должен быть установлен на рабочей станции, на которой будут собираться данные об оргтехнике, а checkcfg можно поместить в доступном для всех пользователей месте в сети. Если с рабочей станции пользователя запустить эту программу, то она, собрав сведения о компьютере, поместит их в файл, из которого эти сведения поступят в программу sklad. Запуская checkcfg с определенной периодичностью, для чего настроив планировщик задач на компьютерах пользователей, не придется даже подходить к их компьютерам для получения обновленных сведений. Вместе с дистрибутивом поставляется очень подробное описание работы с программой. Программа постоянно совершенствуется, последняя версия на момент написания этих строк датирована 30 декабря 2004 года. Если для работы программы потребуется программа BDE (Borland Database Engine, интерфейс доступа к базам данных Borland Database), ее можно закачать с сайта программы учета вычислительной техники бесплатно.

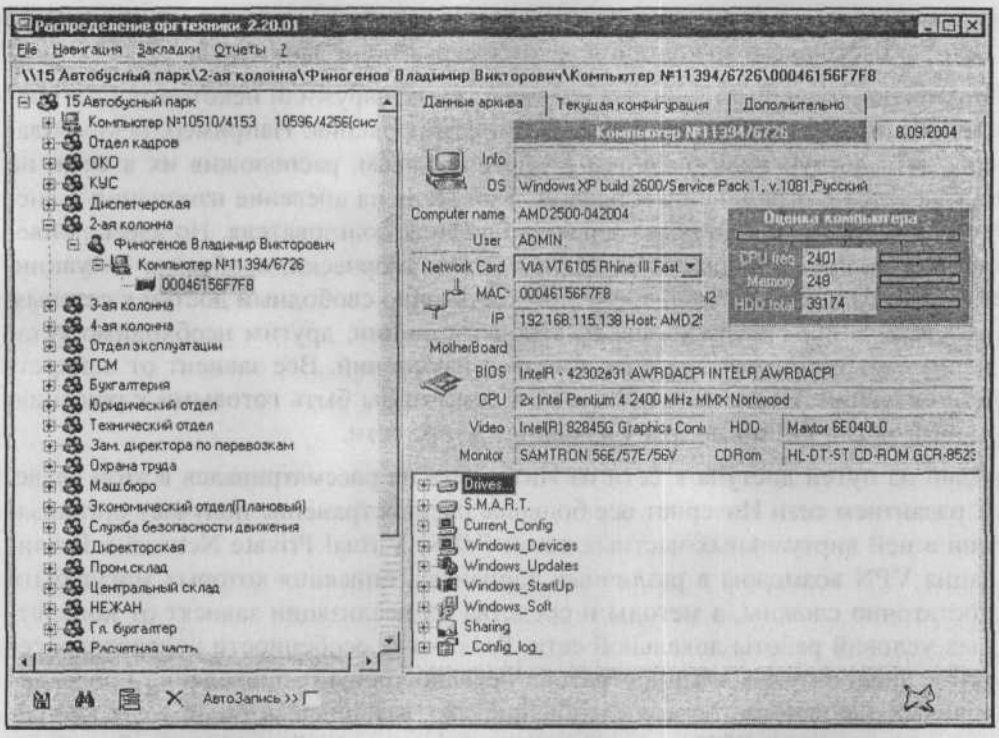

Рис. 5.22. Главное окно программы учета вычислительной техники

Отчеты, формируемые программой, могут быть выведены в формы, текстовые файлы, dbf-файлы, rtf-файлы. Это значит, что работа над информацией, полученной с ее помощью, может продолжаться с помощью средств MS Office или других.

Существуют, разумеется, и другие бесплатные и коммерческие продукты для сбора и учета информации о компьютерной технике. Мы остановили выбор на этой программе, как на самостоятельном инструменте, не требующем дополнительных средств, в отличие от прочих, которые удалось найти в Интернете. Не исключено, что именно вам больше подойдет другая программа для учета компьютерной техники, которую можно найти по адресу **http://www.shatki.info/ox/dnld.php**. Эта программа позволяет вносить сведения вручную. Для автоматизации сбора информации требуется до недавнего времени бесплатная программа AIDA32, к сожалению, ставшей недоступной с июня 2004 года. Ее сменил коммерческий проект EVEREST, а бесплатная версия новой программы (Everest) не согласуется с программой учета. Но если вы имеете опыт программирования на Visual Basic, то на сайте программы доступен ее исходный код. Следовательно, при наличии опыта программирования вы можете подогнать ее под свои требования.

Применение подобных программ позволит вам наладить учет техники, даже если до настоящего времени никто этим серьезно не занимался.

Возможно, что при чтении данной главы вы обнаружили некоторые противоречия в предлагаемых вариантах администрирования. Например, рекомендация дать доступ пользователям к дистрибутивам, расположив их в сети, не согласуется с ограничением прав пользователя на внесение изменений в систему путем настройки обязательного профиля пользователя. Но здесь приведены примеры, которые следует применять творчески, сообразно ситуации. Кому-то из пользователей требуется достаточно свободный доступ к сетевым ресурсам и конфигурации своей рабочей станции, другим необходимо установить жесткие рамки на внесение ими изменений. Все зависит от конкретной ситуации. Наша цель и состоит в том, чтобы быть готовыми к решению любых задач, возникающих у администратора сети.

Один из путей доступа к сети из Интернета не рассматривался в этой главе. С развитием сети Интернет все большее распространение получает организация в ней виртуальных частных сетей (VPN, Virtual Private Network). Реализация VPN возможна в различных вариантах, описания которых могут быть достаточно сложны, а методы и средства их реализации зависят от конкретных условий работы локальной сети. Различные особенности конкретных сетей и предпочтения администратора нередко требуют проведения предварительных экспериментов и исследований. Но, взявшись за такой труд, как администрирование ЛВС, надо быть готовым и к этой кропотливой работе. Применительно к нашей сети и рассматриваемой теме, VPN можно использовать для доступа администратора к серверу или отдельному компьютеру. Подробное описание настройки доступа к сети через VPN приводится в *главе 6*.

ГЛАВА 6

Эксперименты в сети. Особые режимы работы

При наличии Интернета и поисковой системы Google вы можете найти ответы на вопросы и рекомендации практически в любой нестандартной ситуации. Иногда материалы, найденные в Интернете, показывают неожиданно простой путь решения проблемы, а найденные советы бывают очень действенными. Тем не менее не на все вопросы администратора сети можно получить конкретные ответы. Решение многих нестандартных задач требует самостоятельных исследований и экспериментов. Но для проведения эксперимента требуется определенная материальная база. Если у вас нет возможности применить для этого отдельный компьютер, то вы, вероятно, решитесь на использование в этих целях своего собственного или какого-то другого. В то же время, значительные изменения настроек рабочей станции и параметров ее системы потребуют немало времени для их восстановления по окончании эксперимента. Параметры удачной конфигурации системы необходимо подробно записывать, чтобы повторить, когда это потребуется. Все это создает значительные трудности и может мешать текущей работе.

Виртуальный компьютер

Существуют средства, позволяющие иметь в своем распоряжении практически неограниченное число компьютеров для проведения экспериментов. Причем настроенный "компьютер" можно сохранить в архиве, чтобы при необходимости включить его, подробно проанализировать его конфигурацию, сравнив с настройками другого компьютера. Эта роскошь оказывается доступной, если установить на своей рабочей станции виртуальный компьютер. Для этого существует несколько программ различных производителей. В среде любителей поэкспериментировать весьма популярна программа VMware Workstation (**http://www.vmware.com**). Автором применялась программа Microsoft Virtual PC, которая несколько проще в настройке, почти

равноценна по возможностям VMWare и доступна по адресу в Интернете **http://www.microsoft.com/virtualpc**. Компьютеры и диски компьютеров в этой программе — обычные файлы. Сохраняя файлы виртуальных жестких дисков с установленной операционной системой и необходимыми программами, вы можете их в любой момент подключить и получить систему с сохраненной конфигурацией. Применяя определенные меры предосторожности, можно даже испытывать действие вирусов на систему, чтобы своими глазами увидеть симптомы заражения и проверить средства защиты от них. При этом полностью испорченную виртуальную систему можно за несколько секунд заменить заранее сохраненной копией.

Установив программу Virtual PC, вы получите доступ к созданным в ней виртуальным машинам через консоль управления (рис. 6.1).

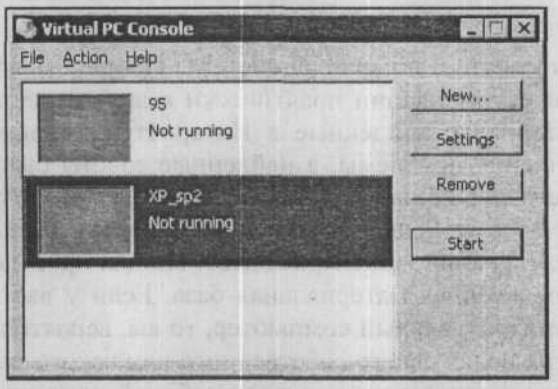

Рис. 6.1. Окно **Virtual PC Console** (Консоль управления виртуальными компьютерами)

Можно создать несколько машин, подготовленных для различных операционных систем. Создав соответствующие виртуальные винчестеры и установив операционные системы, можно сохранить копии файлов виртуальных жестких дисков, обеспечив быстрое восстановление "чистой" системы.

Программа имеет дополнения, которые устанавливаются отдельно и дают возможность использовать общие для основного и виртуального компьютера папки. Настройки виртуальной машины достаточно гибки (рис. 6.2). В качестве периферийного оборудования могут использоваться практически все устройства основного компьютера, кроме модема (это отмечено и в справочной системе данной программы). В случае необходимости можно обеспечить подключение виртуальной машины к Интернету через локальную сеть. При этом локальная сеть может быть реальной или ее имитацией. Для имитации локальной сети между виртуальным компьютером и основной рабочей станцией можно в разъем сетевой карты реальной машины вставить коннектор с отрезком витой пары, у которой обе применяемые пары проводников соеди-

нены перекрестно (1-3, 2-6). При этом если на основном компьютере настроен общий доступ к подключению Интернета, то с виртуальной машины можно получить этот доступ.

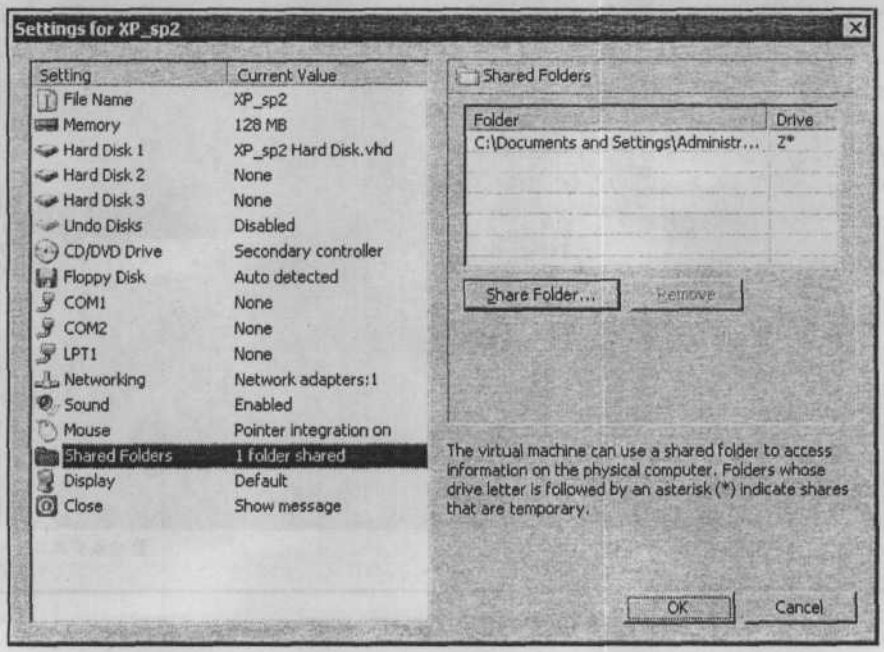

Рис. 6.2. Окно **Settings for XP_sp2** (Настройки виртуальной машины XP_sp2)

Экран виртуальной машины (рис. 6.3) содержит меню для работы с этим экраном, для подключения дисководов и "физического" управления виртуальным компьютером. Функции кнопок включения и перезагрузки переданы соответствующим пунктам меню.

Поскольку для работы виртуального компьютера используются ресурсы реальной машины, то настройки оформления виртуальных систем следует делать "аскетическими", снизив до минимума потребление ресурсов на визуализацию.

Запуская виртуальную машину в вашей сети, учтите, что ведет она себя так же, как и обычный компьютер. Если ее настройки выполнены неверно, например, присвоен IP-адрес, уже существующий в сети, то возникнет конфликт адресов, и работа сети может быть нарушена. Виртуальный компьютер в сети требует к себе такого же отношения, как настоящий.

Используя виртуальный компьютер, вы можете провести эксперименты, необходимые для выявления оптимальных настроек различных сервисов в вашей сети.

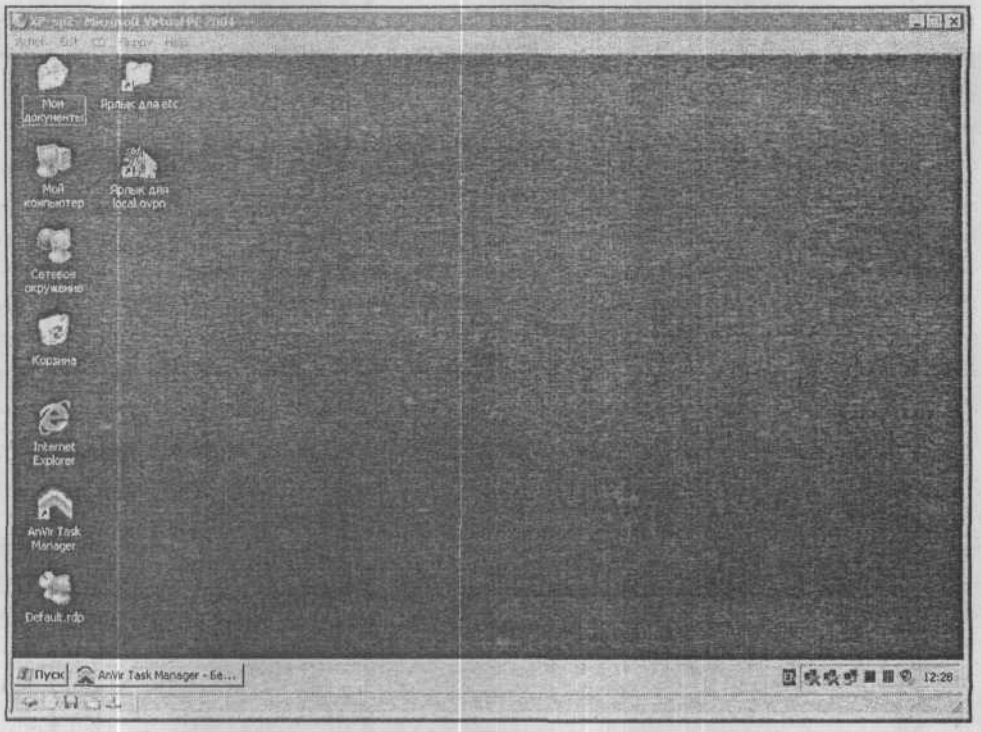

Рис. 6.3. Экран виртуального компьютера

Сохранив копию файла виртуального винчестера после установки ОС и необходимых программ, можно оперативно восстановить первоначальное состояние системы в случае, если эксперименты завели вас в тупиковую ситуацию, и возврат к первоначальным настройкам на обычном компьютере стал весьма трудоемким. Виртуальный компьютер можно использовать и для экспериментов с виртуальной частной сетью (VPN).

Виртуальная частная сеть

Виртуальная частная сеть (Virtual Private Network, VPN) для большинства обычных пользователей и начинающих администраторов — область мало известная. Даже когда услуга по предоставлению виртуальной частной сети обеспечивается какой-либо фирмой (провайдером), то на стороне пользователя обычно производятся настройки клиентской части VPN, что не вызывает затруднений (учитывая рекомендации провайдера). Очень подробное описание настройки VPN для организации связи двух локальных сетей приводится в статье "Конфигурация VPN в Windows 2000" Дугласа Тумбса (Издательство "Открытые системы", **http://www.osp.ru/win2000/worknt/630.htm**).

В статье описано создание виртуальной сети между удаленными локальными сетями, подключенными к Интернету. Но в практике администратора локальной сети чаще может возникнуть задача обеспечения связи одной удаленной рабочей станции с локальной сетью. Организация такого доступа к локальной сети позволяет решить задачу доступа пользователя к своим файлам и принтерам. При этом, в отличие от терминального доступа или доступа через программы удаленного администрирования, на экране компьютера, с которого осуществлен доступ, не будет рабочего стола удаленной машины. Но в сетевом окружении будут необходимые папки, а для печати документов можно использовать принтер, находящийся в локальной сети и подключенный к компьютеру, к которому осуществлен доступ через VPN. Задержки передачи информации между компьютером удаленного пользователя и сетью не повлияют на скорость обычной работы с документами. В зависимости от скорости передачи информации через применяемое подключение к Интернету, будут более или менее значительными время копирования файлов и печати документа. Само по себе соединение устанавливается достаточно быстро даже при использовании выхода в Интернет через обычный модем. У автора соединение устанавливается в течение сорока секунд, в то время как локальная сеть находится на расстоянии более 50 км от места подключения. Единственное условие, которое должно быть соблюдено, — это наличие у рабочей станции, с которой осуществляется доступ к сети, реального (пусть даже динамически выделяемого) IP-адреса, а у компьютера, через который подключена к Интернету локальная сеть, должен быть постоянный IP-адрес, выделенный поставщиком услуг Интернета. Если не ставить условие обратного доступа из сети к удаленной рабочей станции, то подключение может быть выполнено, когда выход в Интернет удаленной рабочей станции выполняется через другую локальную сеть.

Применение VPN позволяет предоставить доступ к файлам и принтерам не только администратору, но отдельным пользователям (возможно, руководителю организации). Доступ к файлам и принтерам через VPN не нарушает работы пользователя компьютера, через который осуществляется доступ. Методы шифрования, применяемые для организации VPN, не позволят постороннему перехватить передаваемую информацию, пароли и получить доступ к сети. В отличие от доступа через сервер терминалов, в данном случае не потребуется и приобретение каких-либо дополнительных лицензий в случае предоставления доступа нескольким пользователям.

Итак, наша сеть через вспомогательный сервер (компьютер) подключена к Интернету через ADSL-модем. Вам требуется доступ к файлам и принтерам сети. Поскольку без экспериментов здесь не обойтись, начнем с описания организации тестовой VPN между двумя машинами. Ваша сеть может сущест-

венно отличаться от той, что рассматривается в данной книге. Поэтому для организации VPN мы воспользуемся свободно распространяемым программным обеспечением, которое может работать на любом компьютере сети, где нет встроенных средств для создания виртуальной сети.

Эта программа называется OpenVPN, а найти ее можно по адресу в Интернете **http://openvpn.sourceforge.net**. Программа распространяется бесплатно, имеет реализации для различных платформ, что позволяет настраивать подключения к серверам, работающим как под Windows, так и под Linux (UNIX). Для скачивания файлов дистрибутива программы лучше воспользоваться страницей **http://openvpn.sourceforge.net/beta**. Серверная и клиентская части программы ничем не отличаются, кроме нескольких строчек в файле конфигурации программы. В режиме сервера программа может быть запущена в качестве службы. После установки программы на компьютере появляется виртуальный сетевой адаптер (рис. 6.4).

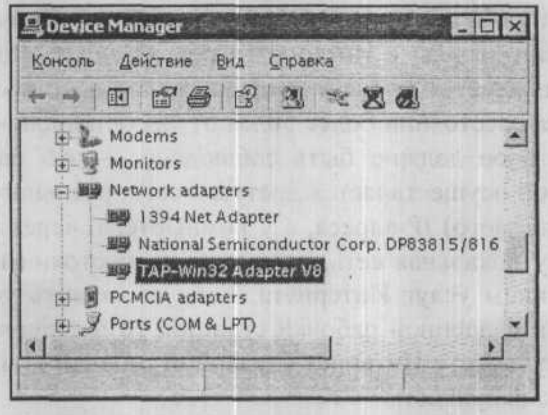

Рис. 6.4. Новый адаптер в перечне оборудования компьютера

Для нового адаптера автоматически создается и новое подключение (рис. 6.5), которое следует сразу переименовать в короткое и понятное имя. Это необходимо, поскольку в файлах конфигурации программы OpenVPN требуется указать имя сетевого адаптера. При этом программа работает в режиме командной строки, где короткие имена предпочтительны.

Файлы конфигурации для сервера и клиента в самом простом варианте приведены в листингах 6.1 и 6.2.

Листинг 6.1. Файл конфигурации для клиента OpenVPN Local.ovpn

```
# имя компьютера, к которому осуществляем доступ
remote hp-admin
```

```
# порт, через который осуществляется связь (любой свободный)
port 35000
# указание на роль компьютера в VPN
proto tcp-client
dev tap
ifconfig 192.168.116.3 255.255.255.0
dev-node vpn
secret key.txt
ping 10
comp-lzo
verb 4
mute 10
```

Листинг 6.2. Файл конфигурации для сервера OpenVPN Server.ovpn

```
port 35000
proto tcp-server
dev tap
ifconfig 192.168.116.1 255.255.255.0
dev-node vpn
secret key.txt
ping 10
comp-lzo
verb 4
mute 10
```

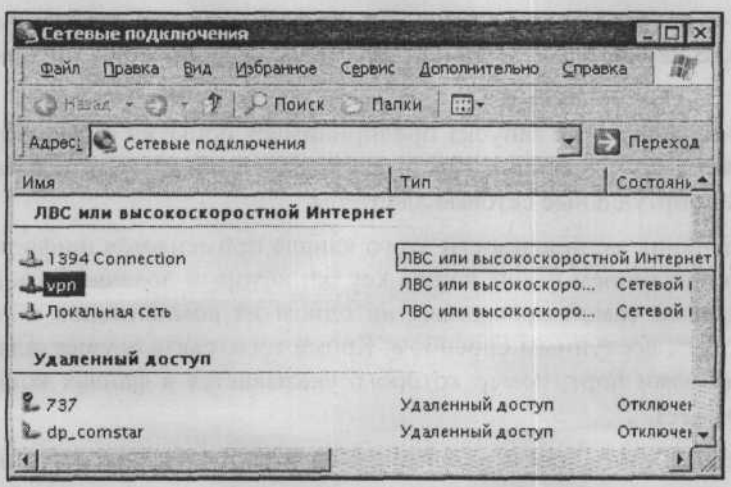

Рис. 6.5. Окно **Сетевые подключения** с новым сетевым подключением

В обоих файлах имя сетевого подключения (dev-node) — "vpn". Сетевые подключения настройки не требуют, их параметры устанавливаются самой программой. Так в клиентском файле есть строка

```
ifconfig 192.168.116.3 255.255.255.0
```

Эта строка устанавливает IP-адрес для подключения VPN равным 192.168.116.3, а маску подсети — 255.255.255.0. Файлы должны иметь расширение ovpn. При этом в контекстном меню этих файлов появится пункт **Start OpenVPN on this config file** (Запустить OpenVPN с этим файлом конфигурации).

Для организации виртуальной частной сети необходимо, чтобы со стороны удаленного компьютера можно было выполнить команду ping по адресу сервера, к которому делается попытка подключения. В локальном файле конфигурации указывается имя сервера (параметр remote), причем это должно быть только имя. Следовательно, связь имени и IP-адреса следует обеспечить одним из доступных способов. Это может быть использование DNS-сервера, который разрешит имя в адрес, или просто запись в файле C:\WINDOWS \system32\drivers\etc\hosts, которая представляет собой строку, содержащую IP-адрес и имя компьютера, разделенные пробелом. В описываемом примере строка в файле Hosts выглядит так:

```
192.168.115.136  hp-admin
```

Адрес в файле Hosts отличается от адреса в файле конфигурации. Это связано с тем, что адрес основного сетевого адаптера не совпадает с адресом адаптера, созданного программой OpenVPN.

OpenVPN-сервер, запущенный на сервере сети, ожидает попыток подключения извне. В случае удачной попытки сетевое подключение VPN активизируется.

OpenVPN-клиент после запуска предпринимает попытки определить доступность сервера по его имени. Как только сервер обнаружен, создается канал связи через виртуальные сетевые адаптеры.

Для обеспечения защищенности этого канала применяется шифрование. Оно реализуется наличием файла ключа key.txt, который должен быть сформирован средствами самой программы на одном из компьютеров и передан на другой любым доступным способом. Кроме того, связь осуществляется через выбранный вами порт, номер которого указывается в файлах конфигурации (параметр port).

Как серверная часть, так и клиентская не имеют графического интерфейса. Работа программы видна в текстовом окне, в котором выводятся все сообщения о действиях программы и ее состоянии. Примеры окон клиентской и сер-

верной частей программы с установленным соединением показаны на рис. 6.6 и 6.7. Признаком установившегося соединения в обеих частях программы является сообщение, содержащее строку — `Initialization Sequence Completed` (Процедура инициализации завершена).

Рис. 6.6. Окно **OpenVPN** на сервере

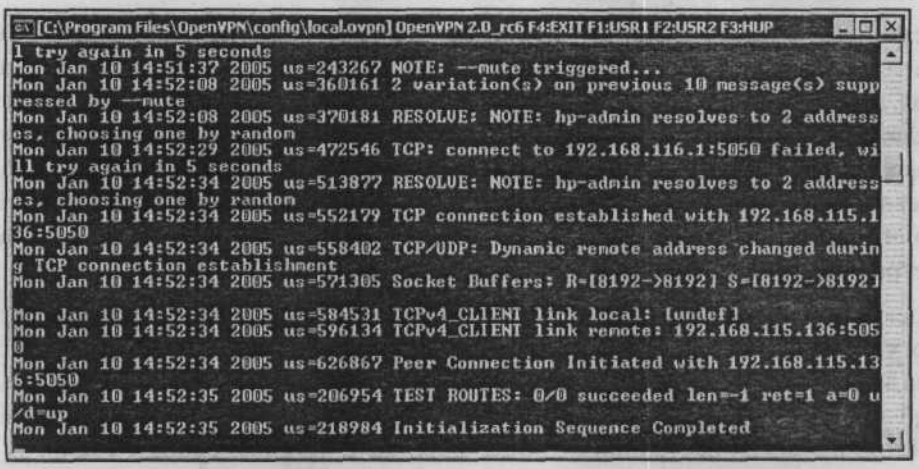

Рис. 6.7. Окно **OpenVPN** на локальной машине

Сообщение клиентской программы `mute triggered` означает, что попытки связи неудачны и программа ожидает изменений в настройках. Например, если был недоступен адрес сервера по его имени, а вы внесли верную запись в файл Hosts (не закрывая OpenVPN), программа возобновит попытки установления связи.

При установившейся связи в сетевом окружении удаленного компьютера появится сервер. Чтобы зарегистрироваться на нем, потребуется ввести имя пользователя и пароль, допустимые в сети.

Для успешного соединения следует проконтролировать выполнение еще двух условий:

- локальный IP-адрес удаленной рабочей станции и сервера должен принадлежать подсети, которой не принадлежат адреса виртуальных адаптеров, созданных OpenVPN;
- имя рабочей группы, к которой принадлежит удаленная рабочая станция, должно совпадать с именем домена или рабочей группы сервера. Компьютер может принадлежать и самому домену (ноутбук, например).

Первое из этих условий обеспечивает однозначность поиска компьютера-сервера программой клиентом. Невыполнение этого условия приведет к невозможности установления связи с удаленной сетью, а OpenVPN не предоставит вам никакой информации о причинах неудачи.

Второе условие обеспечивает появление компьютеров, находящихся в локальной сети, в сетевом окружении удаленной рабочей станции.

При достаточном качестве связи пользователь получит практически все те же возможности, что и при работе в локальной сети.

Если вход в локальную сеть защищен брандмауэром, то необходимо разрешить доступ к файлам и принтерам через виртуальный интерфейс, а основной интерфейс должен быть доступен для команды ping. Для этого следует включить параметр протокола ICMP (Internet Control Message Protocol, протокол управляющих сообщений в сети Интернет) **Разрешать запрос входящего эха**, что обеспечит возможность ответов компьютера на команду ping по его адресу. Настройки этого протокола доступны в дополнительных параметрах брандмауэра в ОС Windows XP и Windows 2003 Server.

Поскольку в каждой сети, в том числе и в вашей, настройки доступа к ней могут иметь свои особенности, без экспериментов вам не обойтись, поэтому для тонкой настройки придется обратиться к справке по OpenVPN и справочной системе Windows. Но применение OpenVPN позволит вам достаточно быстро провести настройки подключения, если они возможны в ваших условиях. Когда подключение установлено, скорость передачи информации по этому каналу будет ниже, чем при прямом соединении. Дополнительные преобразования информации, шифрование и дешифрование, — все это требует добавочного времени. Но для обычной работы в сети скорость связи вполне достаточна, особенно если рабочая станция подключена к Интернету через быстрый канал связи. Автору удалось установить такое соединение через коммутируемый доступ (dial-up). При этом работа с документом Word требо-

вала, чтобы он был скопирован на рабочую станцию, но печать на один из принтеров сети проходила нормально. Более того, этот принтер был подключен к рабочей станции во время соединения. Для ускорения процесса подключения желательно, чтобы драйвер принтера уже был установлен на удаленной рабочей станции.

Можно обеспечить несколько подключений к серверу, запустив на нем несколько экземпляров OpenVPN-сервера. Каждый из экземпляров должен быть связан со своим виртуальным сетевым подключением. Виртуальные подключения могут создаваться средствами OpenVPN в любом необходимом количестве. Это позволяет для каждого подключения применять свой ключевой файл, что повышает защищенность сети.

Описанный выше пример подключения предназначен только для первого опыта его организации. В нем предполагается прямое соединение двух компьютеров перекрестным кабелем или через концентратор (хаб, коммутатор). Реальное соединение, которое далее будет описано, лучше организовывать после удачного завершения первого эксперимента по установке связи между двумя компьютерами. Для реальной связи через Интернет с локальной сетью потребуется более кропотливая работа. Приведем пример реально работающей пары компьютеров, связанных через VPN. Само собой разумеется, что на оба компьютера необходимо установить OptnVPN. Имя виртуальному сетевому адаптеру следует присвоить короткое, латинскими буквами. Можно использовать имя программы OpenVPN.

В этом примере описаны настройки для двух компьютеров. Один из них — ноутбук, который работает и в локальной сети и вне ее. Другой — вспомогательный сервер под управлением Windows Server 2003, через который локальная сеть имеет выход в Интернет. Подключение к Интернету осуществлено через ADSL-модем. При этом сеть имеет единственный внешний адрес 81.195.117.138. Внутренние адреса ЛВС принадлежат подсети 192.168.115.0. Постоянный адрес ноутбука в данном случае значения не имеет, поскольку при подключении к Интернету через обычный модем он получает динамически выделяемый адрес. Конкретное значение этого адреса тоже не имеет значения и в настройках соединения не применяется. В файлах конфигурации OpenVPN виртуальным сетевым адаптерам присваиваются адреса: 192.168.116.1 — для сервера и 192.168.116.2 — для ноутбука (удаленной рабочей станции). На рис. 6.8 схематично показана организация подключения к локальной сети через Интернет с использованием виртуальной частной сети.

Прежде всего, необходимо обеспечить возможность ответа сервера на команду ping. Иногда администраторы намеренно запрещают эту возможность, пытаясь максимально обезопасить сеть от проникновения в нее извне. Но в нашем случае именно такое проникновение и готовится. При этом защищенность сети не ухудшается, если не считать возможности простого обнаруже-

ния вашего компьютера (сервера) из Интернета. Ответ компьютера на команду ping запрещается, если включен брандмауэр и выключен параметр протокола ICMP (Internet Control Message Protocol) **Запрос входящего эха** (рис. 6.9).

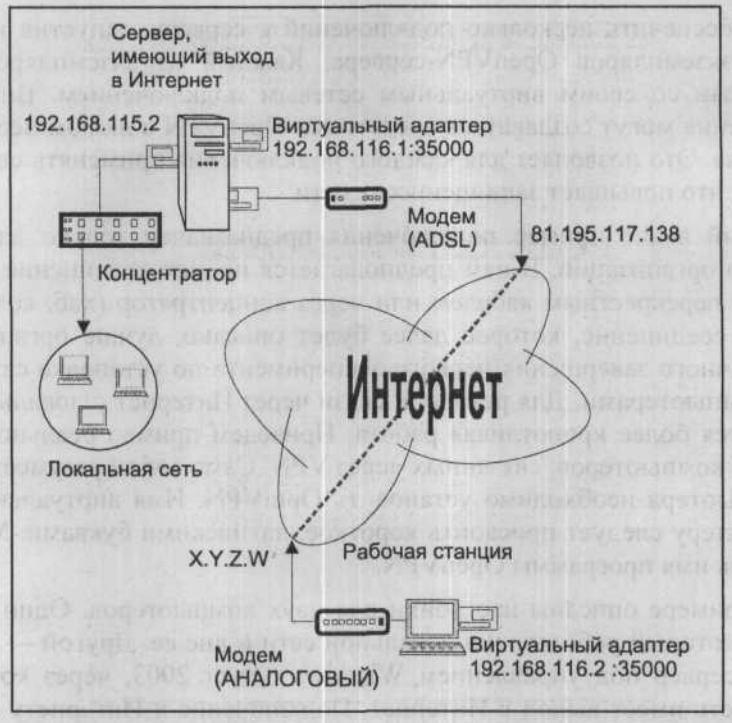

Рис. 6.8. Схема подключения к ЛВС через Интернет с применением VPN

Компьютер, имеющий несколько сетевых подключений (соответственно и несколько сетевых адаптеров), может иметь различные настройки брандмауэра для каждого из них. Тем более это относится к компьютеру, на котором настроено преобразование сетевых адресов (NAT). Поэтому, настраивая параметры сетевых подключений, будьте внимательны. Случайная ошибка при установке параметров подключений к катастрофе не приведет, но заставит помучиться в поисках причин неудачи.

Когда вы убедились, что команда ping до сервера проходит нормально, время ответа не превышает 300 мс, а разброс значений этого времени невелик (не более 50 %), можно продолжать настройки. Если время ответа больше, работа с удаленной рабочей станции с ресурсами локальной сети будет очень медленной. Но иногда достаточно даже медленной связи для выполнения необходимых процедур администрирования. Связь будет очень неустойчивой,

если ответы на команду ping будут нерегулярными. В случае появления среди строчек ответов на экране сообщения Превышено время ожидания следует искать причины нарушения качества связи или выбрать другое время для подключения.

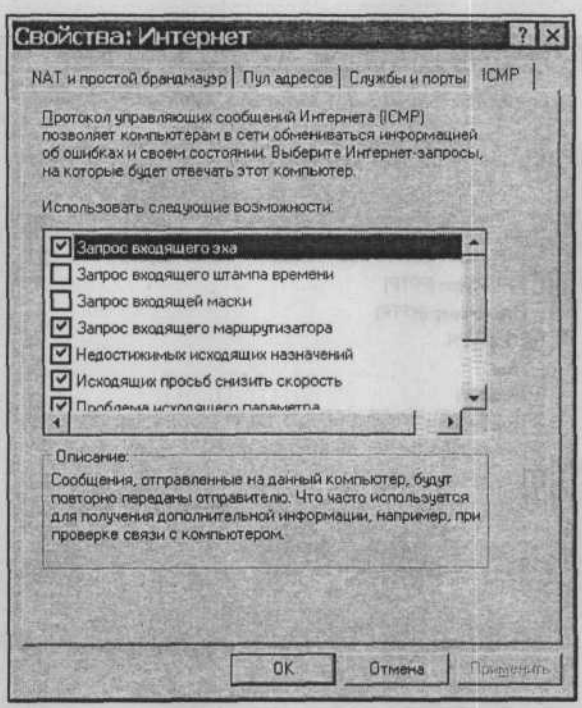

Рис. 6.9. Свойства интерфейса "Интернет", настройка ICMP (**Запрос входящего эха**)

Защищенный канал связи, создаваемый в Интернете, работает через порт, который мы зададим в файлах конфигурации OpenVPN. Это значит, что на всем протяжении этого канала (Рабочая станция—сервер провайдера1—Интернет—сервер провайдера2—сервер локальной сети) данный порт должен быть открыт. В примере показано применение порта 35 000, но можно выбрать любое значение, не используемое на вашем сервере. Если есть сомнения в том, что выбранный вами порт открыт на каком-либо участке предполагаемого канала, его можно изменить. Если на сервере ЛВС не применяется какой-нибудь из известных сервисов, например POP3, то можно использовать стандартный для этого сервиса порт 110. Скорее всего, он будет открыт на всем протяжении канала VPN. Для того чтобы открыть этот порт на вашем сервере, следует настроить свойства интерфейса, подключенного к Интернету в оснастке **Маршрутизация и удаленный доступ**. На рис. 6.10 показано окно **Свойства: Интернет** с перечнем служб, доступных из Интер-

нета. На рис. 6.11 показано окно изменения свойств службы с указанием на номер входящего и исходящего порта. Можно выбрать эти значения разными. В этом случае соответствующие значения должны быть указаны в файлах конфигурации на удаленной рабочей станции (значение для входящего порта) и на сервере (значение для исходящего порта).

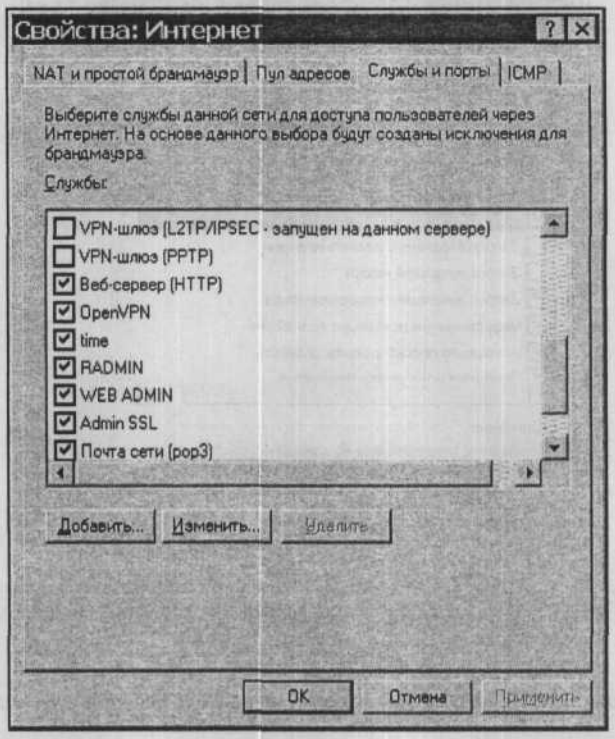

Рис. 6.10. Окно **Свойства: Интернет** с перечнем служб, доступных из Интернета

Открыв используемый порт, необходимо настроить маршрутизацию IP-пакетов, передаваемых через Интернет. Это также делается в оснастке **Маршрутизация и удаленный доступ**, где необходимо указать статические маршруты (рис. 6.12). Один маршрут уже был указан, когда настраивался доступ к Интернету для пользователей сети. Теперь следует добавить еще два (один для основного, другой для виртуального сетевого адаптера).

В дальнейшем может понадобиться подключение других пользователей через VPN. Для этого потребуется создать несколько виртуальных адаптеров по числу создаваемых каналов и присвоить им имена с различными суффиксами. Причем для каждого канала следует запускать свой экземпляр OpenVPN-сервера, а в файле конфигурации каждого экземпляра указать соответствующее имя адаптера. Выбранный вариант маршрутов изменять не потребуется.

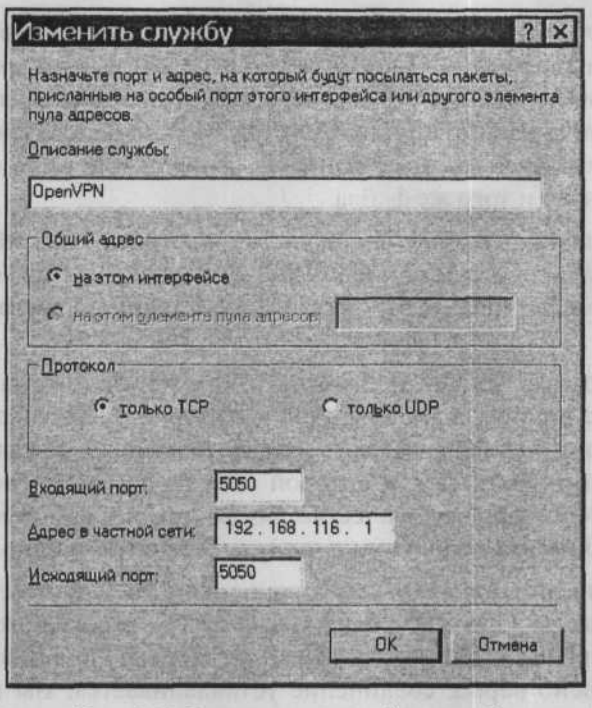

Рис. 6.11. Окно изменения свойств службы

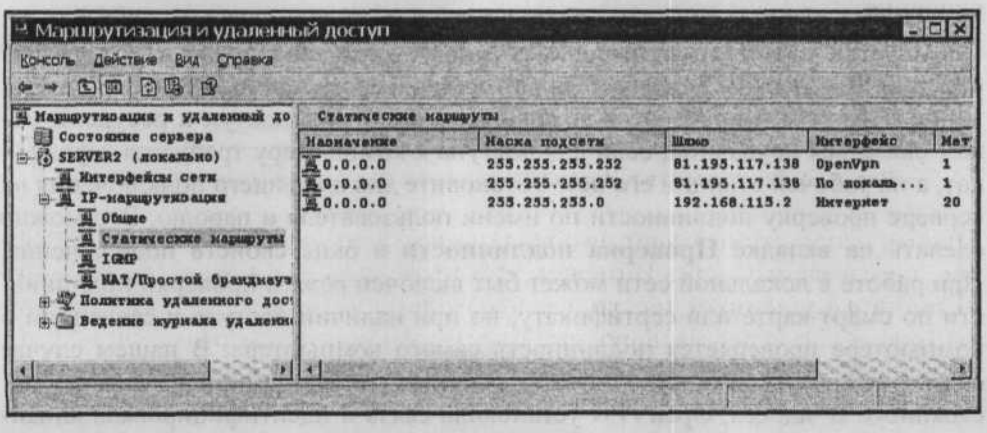

Рис. 6.12. Окно **Маршрутизация и удаленный доступ (Статические маршруты)**

Создадим файлы конфигурации подобные тем, что приведены выше (листинги 6.1 и 6.2), но содержащим новые значения IP-адресов и портов, которые вы будете использовать.

Создадим файл секретного ключа с помощью пункта меню программы OpenVpn **Generate a static OpenVPN key** (Создать статический ключ) и поместим одну копию на OpenVPN-сервере, а другую — на OpenVPN-клиенте в папке с файлами конфигурации программы. Можно использовать и те файлы, что применялись на локальных машинах. Важно, чтобы на обеих машинах были копии одного и того же файла.

На рабочей станции обычно специальных настроек не требуется. Должна быть установлена программа OpenVPN, а в папку с конфигурационными файлами программы помещены файл конфигурации клиента и секретный ключ.

Теперь можно запустить OpenVPN-сервер и попытаться установить соединение с рабочей станцией, подключенной к Интернету. Хорошо, если для проведения пробного подключения есть второй телефон. К сожалению, соединение dial-up по той же линии, к которой подключен ADSL-модем, не всегда бывает достаточно хорошего качества, но, возможно, вам повезет, и вы сможете для эксперимента использовать одну телефонную линию.

На рабочей станции устанавливаем соединение с Интернетом через обычный модем и запускаем OpenVPN с использованием локального (клиентского) файла конфигурации. Программа делает несколько попыток соединения и, если все настроено верно, соединение устанавливается. Вы можете определить момент установки соединения по сообщению `Initialization Sequence Completed`. В противном случае следует проверить настройки и качество соединения.

После установления соединения VPN откройте сетевое окружение на рабочей станции. Вы должны увидеть компьютер, к которому производилось подключение. Попытка открыть этот компьютер и получить доступ к ресурсам может оказаться неудачной, если для доступа к компьютеру требуется сертификат, а на рабочей станции его нет. Установите для входящего подключения на сервере проверку подлинности по имени пользователя и паролю. Это можно сделать на вкладке **Проверка подлинности** в окне свойств подключения. При работе в локальной сети может быт включен режим проверки подлинности по смарт-карте или сертификату, но при наличии доступа к сведениям о компьютере проверяется подлинность самого компьютера. В нашем случае связь оказывается односторонней. Удаленная рабочая станция не имеет постоянного IP-адреса, OpenVPN установила связь и идентифицировала клиента по своему секретному ключу, а сервер теперь хочет проверить подлинность пользователя или компьютера при попытке доступа к его ресурсам. В этом случае можно установить проверку подлинности по имени пользователя и паролю. (На некоторых компьютерах это соответствует выбору метода проверки MD5-Challenge; более понятное наименование метода может отсутствовать.)

Можно, конечно, установить и настроить центр сертификации на сервере Windows server 2003. Но это тема отдельного разговора.

Подключение к рабочим станциям сети

Если вам удалось подключиться к серверу сети или к к компьютеру, имеющему непосредственное подключение к Интернету, то можно начинать настройку доступа к любой рабочей станции сети (рис. 6.13). Эта возможность позволяет любому пользователю (если вы настроили для него доступ) подключиться из дома к своему рабочему компьютеру. В нашей сети второй сервер, имея непосредственное подключение к Интернету, имеет реальный IP-адрес в Интернете. Другие компьютеры сети имеют только внутренние адреса. Тем не менее есть возможность обеспечить доступ к этим компьютерам через VPN. Это возможно, потому что обращение к компьютерам происходит не только по IP-адресу, но и с использованием определенного порта. Если на стороне OpenVPN-клиента в файле конфигурации указать порт, отличающийся от того, который был применен для связи с сервером, а на сервере, подключенном к Интернету, создать маршрут к рабочей станции в локальной сети, OpenVPN-сервер на которой имеет этот же номер порта, то связь OpenVPN-клиента осуществится именно с этой рабочей станцией. Если применяется брандмауэр, то необходимо разрешить доступ из Интернета по этому номеру порта.

Настройте доступ по выбранному порту к рабочей станции, создав еще одну запись для службы OpenVpn подобно тому, как показано на рис. 6.10, но с именем, отличным от существующего (например, OpenVpn1), адресовав ее на соответствующий рабочей станции IP-адрес и указав выбранный для работы порт. Следует указать также статические маршруты (рис. 6.12) к рабочим станциям. Указывать их надо для интерфейса, подключенного к Интернету. Шлюз — адаптер, смотрящий в локальную сеть, назначение — IP-адрес рабочей станции в сети, маска подсети — 255.255.255.255.

Можно заранее настроить возможность доступа к нескольким рабочим станциям, выбрав для них различные номера портов. Если при организации удаленного доступа пользователя к своей рабочей станции подготовить отдельный ключевой файл, то кроме этого пользователя никто не сможет подключиться к его рабочей станции. Аналогично, этот пользователь не сможет подключиться к другим рабочим станциям и серверам.

При подготовке нескольких подключений следует дать понятные имена ключевым файлам, самим подключениям и файлам конфигурации, чтобы избежать путаницы.

Если ваш компьютер (рабочая станция) поддерживает работу с несколькими сетевыми адаптерами, то можно одновременно подключиться к рабочей

станции в локальной сети и к серверу. Несмотря на то, что в файлах конфигурации клиентов будет указано одно и то же имя удаленного компьютера, соответствующее IP-адресу сервера, подключение будет происходить к соответствующим рабочим станциям. При этом в сетевом окружении они будут появляться под своими именами. Таким образом, ваша работа на удаленной рабочей станции почти не будет отличаться от работы в локальной сети. Работу с несколькими виртуальными сетевыми адаптерами необходимо обязательно проверить в условиях, когда с одним адаптером все работает устойчиво. Если вместо сообщения `Initialization Sequence Completed` на экране

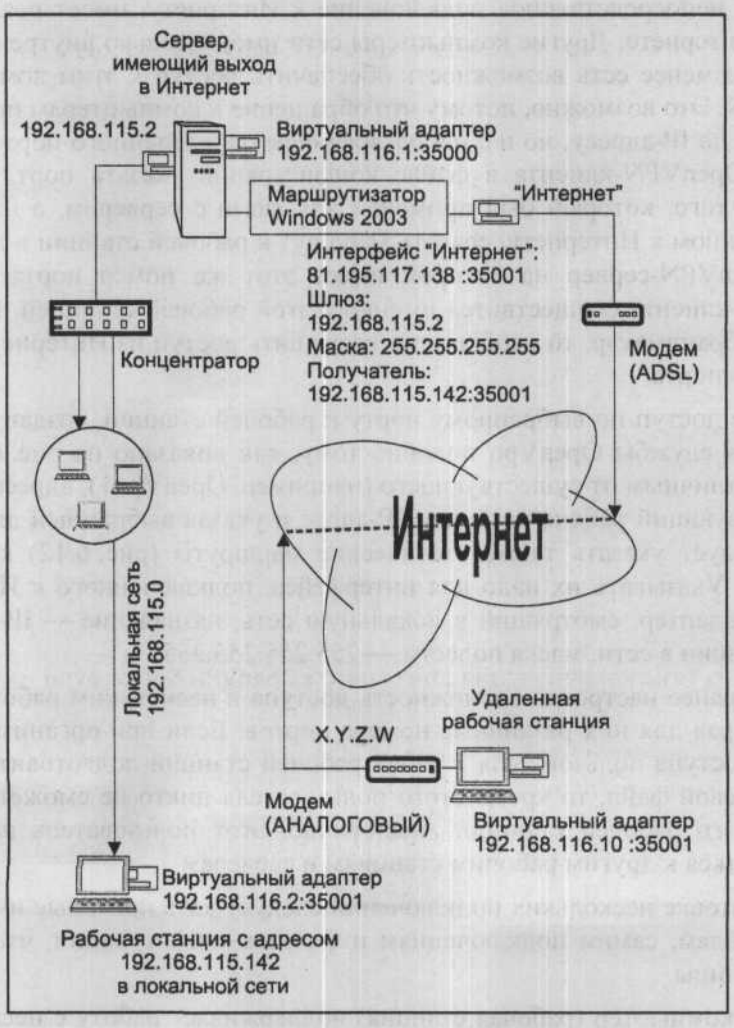

Рис. 6.13. Схема подключения к рабочей станции

будет появляться `Initialization Sequence Completed with Errors`, когда установлено более одного виртуального адаптера, работа с сетевыми ресурсами может быть затруднена или невозможна.

В файлах конфигурации могут быть предусмотрены параметры, позволяющие улучшить надежность VPN-соединения и уменьшить время его восстановления при сбоях. Подробное описание всех возможных параметров приведено на сайте разработчиков OpenVPN, а здесь приведем еще раз содержимое файлов конфигурации сервера и клиента с некоторыми изменениями (листинги 6.3 и 6.4).

Листинг 6.3. Файл конфигурации для клиента OpenVPN Local.ovpn

```
remote server2 # необходимо в файле HOSTS указать IP-адрес
proto tcp-client
dev tap2
ifconfig 192.168.116.12 255.255.255.0
mssfix
dev-node den
secret den.txt
ping-restart 60
ping-timer-rem
persist-key
resolv-retry 86400

ping 10
comp-lzo
verb 4
mute 10
```

Листинг 6.4. Файл конфигурации для сервера OpenVPN Server.ovpn

```
port 35001
proto tcp-server
dev tap
ifconfig 192.168.116.142 255.255.255.0
dev-node <Имя подключения>
secret den.txt
ping 10
comp-lzo
verb 4
mute 10
```

В обоих файлах (один клиентский, другой серверный) упоминается один и тот же файл ключа (копия). При этом имя ключевого файла можно изменять.

Если вам все удалось и вы довольны результатом, — не торопитесь считать работу завершенной. Возможно, что вы не заметили наличие "подводных камней".

О возможных проблемах и реальных перспективах

Несмотря на удобство доступа к компьютерам сети по через VPN и защищенность канала связи, после удачно организованного доступа к сети не спешите вводить этот метод удаленной работы в "промышленную эксплуатацию". Это относится в равной мере ко всем новшествам, применяемым в вашей сети. Вполне может случиться, что новая программа или устройство, в том числе и виртуальное, станет конфликтовать с другими компонентами системы. Если обнаружится, что OpenVPN не уживается с какой-либо программой или службой, следует попытаться найти причины конфликта. Если это не удается, то можно попытаться разделить во времени конфликтующие процессы. Такие конфликты особенно вероятны, когда процессы запускаются на сервере. В нашей сети, например, при запуске OpenVPN на сервере пропадает удаленный доступ к одной из баз данных, обслуживаемых разработчиками только в режиме удаленного доступа. Возможны некоторые нарушения в работе локальной сети. Но все эти проблемы могут быть успешно решены. Важно внимательно отнестись к анализу работоспособности сети, попытаться в короткое время получить максимум сведений о состоянии системы. Если не замечено никаких проблем, связанных с применением VPN, то начинайте использовать эту возможность в повседневной работе. Тем не менее, если вы решили получать доступ к рабочей станции, нет смысла оставлять работающей OpenVPN, когда вы находитесь непосредственно около этого компьютера. Для сервера можно рассмотреть возможность запуска программы только при необходимости с помощью средств удаленного администрирования или через планировщик задач. Если конфликтов не обнаружено, то OpenVPN может быть запущена постоянно. Ресурсы, которые требуются программе, для современных компьютеров незначительны.

Обычно конфликтов не наблюдается, когда осуществляется доступ пользователя к своей рабочей станции, и при этом никто более не работает за этим компьютером.

Следует учитывать, что проект OpenVPN активно развивается. В то время, когда вы читаете эту книгу, по адресу **http://openvpn.sourceforge.net** уже доступна новая версия программы. Появилась возможность к одному VPN-серверу подключать несколько клиентов, можно применить маршрутизацию

с локальной сетью. Специально для работы в ОС Windows XP Sp 2 добавлена возможность объединения подключений OpenVPN в мост (упрощенный вариант маршрутизации). Уже сейчас программа OpenVPN позволяет организовать связь с компьютерами, работающими в разных сетях, имеющих выход в Интернет. При этом в одной из них может не быть компьютеров с реальными IP-адресами, как при подключении Dial-up, например, а большинство портов интерфейсов, выходящих в Интернет, закрыты сервером с NAT или прокси-сервером (должен быть обязательно открыт лишь порт OpenVpn-соединения). Во многих домашних (городских, районных) сетях доступ в Интернет организован через VPN. Это тоже не помеха для OpenVPN. До момента, когда каждый компьютер сможет иметь свой IP-адрес, а это произойдет после внедрения протокола IPv6, OpenVPN будет помогать компенсировать отсутствие реального IP-адреса у вашего компьютера благодаря технологиям, примененным при разработке этой программы.

Вспомогательные программы на дискетах

В последнее время изготовители компьютеров пытаются продавать машины, не имеющие приводов для гибких дисков. Во многих случаях это оправдано тем, что распространение электронной почты позволяет передавать файлы на любое расстояние, а для временного хранения применяются подключаемые внешние носители, имеющие компактную конструкцию и существенный объем памяти. Тем не менее не всегда надежные по современным меркам и не слишком вместительные "флоппики" со счетов сбрасывать нельзя. Администрируя сеть, приходится сталкиваться с локальными проблемами, когда сеть не может помочь машине, потерявшей к ней доступ, и вообще потерявшей возможность самостоятельно загружаться. В этот момент совершенно незаменимы программные средства, имеющиеся у администратора на дискетах. Таких средств уже создано (и может быть создано самим администратором) очень много. Это и обычные загрузочные дискеты, и дискеты со специальными программами, которые могут выручить во многих нестандартных ситуациях. Опишем некоторые из таких специальных дискет, применяемых довольно редко, но способных оказаться незаменимыми в отдельных случаях.

"Портативный" Web- и FTP-сервер

Иногда для проверки возможностей клиентского программного обеспечения в сети необходимо иметь доступ к FTP- или Web-серверу. Бывает также, что дистрибутив операционной системы хранится у вас в сети, а компьютер, на который требуется установить ОС, не имеет дисковода для CD-дисков и работающего подключения к сети. Особенно вероятны такие ситуации, когда

приходится иметь дело с устаревшей, но еще работающей в сети техникой. В таких случаях можно применить Web/FTP-сервер на одной дискете! Пользователи локальной сети могут через любой Web-браузер или FTP-клиент обратиться к ресурсам того компьютера, где запущен описываемый сервер. FTP-сервер позволяет закачать на компьютер файлы, которые иным способом записать на жесткий диск не представляется возможным. Дистрибутив Web/FTP-сервера на одной дискете можно найти по адресу **http://386.eznos.org/** или воспользоваться файлом diskwww.zip (**www.okobox.narod.ru**), содержащим образ дискеты и программу diskdupe.exe, позволяющую преобразовать этот образ в рабочую дискету. Последняя включает почти все необходимое для запуска сервера на машинах, начиная с процессора 80386, но, в отличие от оригинальной, она содержит операционную систему MS-DOS 7 (русифицированную), и при старте на экране появляется сообщение о запуске Windows 98. Учтите, каким бы дистрибутивом вы не воспользовались, все равно придется настраивать сервер в соответствии с параметрами сети и применяемым сетевым адаптером.

Настройка сервера несложна, но требует внимания.

Она заключается в изменении записей в файлах конфигурации. Прежде всего, заглянем в файл a:\nos\autoexec.nos. Как и другие подобные файлы сервера, этот текстовый файл можно редактировать любым текстовым редактором. На дискете, полученной из образа архива diskwww.zip, уже есть необходимый редактор (edit.com), который известен практически всем пользователям ПК, когда-либо работавшим в среде MS-DOS. Далее (листинги 6.5—6.7) приведено содержание данного и других файлов из архива diskwww.zip. Для тех, кто будет пользоваться прочими дистрибутивами, эти описания также подойдут — отличия не принципиальны.

Файл Autoexec.nos

Файл Autoexec.nos (листинг 6.5) содержит основные настройки сервера. Сразу отмечу, что символы "#" или "rem" предваряют все комментарии и неисполняемые команды.

Листинг 6.5. Файл Autoexec.nos

```
# ============
# autoexec.nos
# ============

hostname webbserver #Имя вашего сервера.
ip address 192.168.0.111 #IP-адрес сервера должен быть заменен на другой,
#допустимый в вашей сети.
```

```
#Следующие значения параметров TCP/IP лучше не изменять, если вы не
#знаете, зачем это делаете.
tcp mss 1460
tcp window 4096
tcp syn off
tcp maxwait 60000
tcp irtt 1000
tcp timer linear
ip ttl 50
isat 1

attach packet 0x62 en0 5 1500
#Данная команда подключает пакетный драйвер вашей сетевой платы. На
#рабочей дискете есть драйверы для двух плат, с которыми проверялась
#работа сервера.
# Устанавливать прерывания обычно не требуется, но если устройства
#конфликтуют, компьютер придется настроить. Если не знаете как, то
#обратитесь к опытным пользователям или доступным описаниям.

route add 192.168.0/24 en0
#Маска подсети. Возможны варианты 192.168/16; 172.16/16; 10/8. Если
#возникают трудности с определением маски подсети в этом формате, то на
#дискете в каталоге WWW можно воспользоваться файлом Netmask.htm.

route add default en0 192.168.0.15
#Адрес вашего маршрутизатора или основного сервера.
# Add domain name server
#Замените адреса в следующих двух строках значениями, соответствующими
#используемым вами DNS-серверам. Если таких нет или вы не хотите их
#применять, то не удаляйте #символ комментария перед этими строками:
#domain addserver 192.168.0.15
# domain addserver 192.168.1.254

# ===Start Services===
# FTP services

#Для работы FTP-сервера необходимо сохранить записи о пользователях
в #файле ftpusers.
#Следующие четыре строчки можно не изменять.
ftype image
ftptdisc 900
ftpmax 10
start ftp
#Сервер может использовать страницы как с дискеты, так и с жесткого
#диска, если он есть. Для настройки запуска с применением порта 80 и
#каталога документов c:\nos\www следует написать:
#start http 80 c \nos\www (после буквы диска двоеточие не ставить).
```

```
#Измените следующую строку в соответствии с этим описанием:
start http 80 a \www
#В следующих двух строках приведены варианты настройки выключения (exit)
#или перезагрузки (reboot) сервера. Автор рекомендует перезагружать его
#ежедневно, однако сервер может работать и без перезагрузки.
#Параметр 0500 обозначает время в часах и минутах.

# at 0600 exit
at 0500 reboot
```

Файл HTTPD.BAT

Файл HTTPD.BAT (листинг 6.6) содержит указание на используемый пакетный драйвер, который должен быть помещен в каталог a:\NOS\BIN. В этом файле строки с комментариями и неисполняемыми командами начинаются с REM, как и в обычных bat-файлах.

Листинг 6.6. Файл HTTPD.BAT

```
@echo off
REM Настройка сети. Оба драйвера есть на дискете. Если у вас установлена
REM другая сетевая плата, то возьмите ее пакетный драйвер с дискеты,
REM прилагающейся к плате, или найдите в Интернете. В строке указывается
REM только имя файла без расширения, 0x62 пропускать нельзя.
rem \nos\bin\Rtspkt 0x62
\nos\bin\Hppclanp 0x62
REM Старт сервера
\nos\bin\nos.exe -f\nos\nos.cfg
REM Отключение от сети при выключении сервера
\nos\bin\termin 0x62
echo\
```

Файл Ftpusers

В файле A:\NOS\Ftpusers (листинг 6.7) представлены настройки доступа к FTP-серверу. Именно с его помощью удобно загружать необходимые файлы на компьютер из сети. Этот файл не имеет расширения.

Листинг 6.7. Файл Ftpusers

```
admin parol \ 127;ftp\user 127;ftp\univ 127
univperm * c:\doc 3
user secret c:\arx 7
```

Цифры обозначают уровень доступа:

- `1` — только чтение;
- `3` — чтение и запись без возможности удаления;
- `7` — полный доступ;
- `127` — системного администратора;
- `128` — запрещение доступа.

Формат записи разрешений доступа в общем случае выглядит так:

```
<Пользователь><Пароль>[Буква диска:] \<Путь1>
<Доступ>;\<Путь2><Доступ>.
```

Звездочка обозначает пустой пароль. Буква для диска "A:" может быть опущена. С настройками, приведенными здесь, сервер может работать в сети с адресом основного сервера — 192.168.0.15 и маской подсети 255.255.255.0. Причем вход через браузер будет всегда обеспечен с любой рабочей станции. Для предоставления доступа берется числовой формат IP-адреса **http:// 192.168.0.111**, а для доступа к FTP нужно ввести `ftp:// имяпользователя@192.168.0.111`. Пароль будет запрошен автоматически, но его можно ввести сразу же в адресе:

```
ftp:// имяпользователя:пароль @192.168.0.111.
```

При удачном соединении с сервером на экране компьютера, с которого устанавливалось соединение, появится страница приветствия: на русском языке — для описываемой дискеты, на английском — для оригинальных файлов.

Краткий список команд для управления сервером

Операционная система, в среде которой работает сервер, и сам сервер имеют лишь текстовый режим. Команды, вводимые с клавиатуры, позволяют управлять сервером, а также получать некоторую информацию о его работе. Возможен вызов сеанса DOS для выполнения каких-либо операций с файлами. Вызов сеанса DOS не приостанавливает работу сервера. Основные команды управления сервером приведены ниже.

- `?` — вывод перечня команд на экран;
- `cls` — очистка экрана;
- `exit` — закрытие (выключение) сервера;
- `help` — помощь;
- `http status` — статус сервера;
- `info` — информация о сервере;

- `multitask on` — включение многозадачного режима (в этом режиме можно работать на рабочей станции с установленным и запущенным сервером);
- `ping w.x.y.z` — ping по сетевому адресу;
- `pkstat` — детализация трафика;
- `route` — вывод таблицы маршрутизации на экран;
- `shell` — сеанс DOS, для возврата — `exit`.

После однократной настройки сервера на дискете вы сможете применить его на любом компьютере, изменив лишь драйвер сетевой платы, если это необходимо. Быстродействие сервера невелико, но для первоначальной загрузки файлов дистрибутива операционной системы вполне достаточно.

Если в вашем распоряжении есть старые компьютеры, которые уже невозможно применить для работы пользователей в сети, вы можете их использовать для организации Web/FTP-серверов, где могут храниться полезные файлы, а на страницах Web-серверов полезная для пользователей информация. Такие серверы не требуют обслуживания и могут работать круглосуточно.

Примечание

Попытка запуска такого сервера на виртуальном компьютере или на современном ноутбуке вероятнее всего приведет к неудаче. Не ко всем новым сетевым адаптерам изготовители дают пакетный драйвер. Для запуска сервера на новых компьютерах можно применить сетевой адаптер, к которому уже найден пакетный драйвер (файлы пакетных драйверов имеют расширение COM).

Аварийный доступ к диску

Несмотря на надежность современных операционных систем и совершенство антивирусных программ, случаются ситуации, когда сбой в системе приводит к невозможности запустить ее. Доступ к диску оказывается закрыт. Восстановление системы возможно, когда к нему заранее готовились, иначе даже загрузка с помощью консоли восстановления в Windows XP во многих случаях не приводит к желаемому результату. В таких случаях возникает огромное желание просто получить доступ к документам, скопировать их на внешний носитель и переустановить систему. Если с переустановкой системы проблем обычно не возникает, то получение доступа к диску с файловой системой NTFS или NTFS5 без специальных средств оказывается невозможным. Сама операционная система Windows XP задумана таким образом, чтобы максимально защитить файлы на жестком диске от несанкционированных изменений. Как обычно, выход из такой ситуации будем искать у сторонних разработчиков программного обеспечения.

На просторах Всемирной паутины можно обнаружить немало интересных и полезных разработок. Каждый раз при возникновении каких-либо проблем мы ищем варианты их решения в Интернете. Вот и на этот раз, когда возникла аварийная ситуация (система перестала загружаться), несмотря на уже имеющиеся средства для выхода из создавшегося положения, попробуем посмотреть, что же нового появилось в Интернете по этому вопросу. Результаты поиска оказались весьма интересными.

На сайте **http://www.remont-pc.ru/** содержится информация о комплекте спасательных дискет. С дискет этого комплекта можно получить доступ к любой файловой системе в текстовом режиме.

Это значит, что в критической ситуации, когда система не загружается, и мы не видим способа восстановить ее работоспособность, нам следует загрузиться с этих дискет и скопировать файлы, требующие сохранения, на внешний носитель. Можно также выполнить исправления на жестком диске, если вы знаете, что следует исправить. Во всяком случае, у вас всегда есть надежда на сохранение важных данных в случае серьезных проблем с ОС и необходимости ее переустановки.

Разработчики комплекта живут в России. Разработка не бесплатна, но ее цена доступна каждому. Автор приобрел комплект дискет за 200 рублей.

При загрузке с этих дискет вы получите полный доступ к томам NTFS, возможность редактирования текстовых файлов, а также выполнения различных процедур с дисками и файлами.

Кроме доступа к диску, этот комплект дискет позволяет получить доступ к реестру Windows, причем для всех применяемых сейчас ОС. Есть на этой дискете средства для работы с дисками.

Примечание

Загрузка виртуального компьютера с этих дискет бессмысленна. Виртуальный компьютер имеет виртуальный винчестер. Обращения программ комплекта должно производиться к реальному физическому диску.

Загрузочная дискета с доступом к сети

На странице **http://www.nu2.nu/bootdisk/network/** есть информация о другой дискете, предназначенной для аварийных ситуаций. Эта дискета имеет очень интересную особенность: при загрузке с нее можно получить доступ к сети! Причем в полноценном режиме, когда можно зарегистрироваться доменным пользователем и получить доступ ко всем разрешенным ресурсам сети. При наличии такой дискеты вы получаете возможность копировать важные данные в сетевой каталог, что часто значительно удобнее, чем сохранение копии на внешнем носителе. Не менее полезно и то, что можно обращаться к дист-

рибутивам, которые находятся в сети, копируя их на локальную машину. Дискета распространяется бесплатно!

Описанная дискета после создания уже содержит некоторое число драйверов сетевых адаптеров. Но при необходимости вы можете загрузить дополнительные драйверы с сайта авторов дискеты, дополнив уже существующий комплект. При загрузке с дискеты установленный сетевой адаптер может быть определен автоматически. Имеющийся на дискете комплект драйверов достаточен с большой степенью вероятности.

Наиболее простой путь создания дискеты — скачать архив BFD full package v1.0.7 (1.45MB). Это архив файлов, достаточный для создания работоспособной дискеты.

Распакуйте архив в любой каталог, измените расширение файла bfd.sam на bfd.cfg.

Из командной строки запустите на выполнение файл bfd.cmd с параметром `msnet: bfd msnet`.

Следуйте командам на экране.

Вот и все. Дискета готова.

На дискете уже присутствуют в упакованном виде файлы Volkov Commander. Для того чтобы программу можно было запустить после загрузки с дискеты, добавьте в Avtoexec.bat после метки `_skipcp` следующие строки:

```
if not exist %srcdrv%\lib\vc.cab goto :_notvc
extract /y /l %ramdrv%\ /e %srcdrv%\lib\vc.cab
:_notvc
```

Следующая строка файла:

```
set path=%ramdrv%\bin;%ramdrv%\
```

После такого редактирования вы сможете запустить файловый менеджер командой `vc`.

После первой загрузки программа предложит внести данные сетевой конфигурации. При этом можно сохранить в различные профили варианты загрузки с различными подключениями к сетевым дискам, например. К сожалению, вам не удастся использовать эту дискету для подключения к компьютерам с Windows XP или Windows Server 2003 . Но к Windows 2000 Server, а также к машинам с Windows 98 и Windows 2000 подключение происходит успешно. Если в вашей сети основным является Windows 2000 Server, то при необходимости вы сможете к нему подключаться и скопировать нужные файлы. Правда, есть здесь и ложка дегтя: при загрузке с этой дискеты нет доступа к томам NTFS на локальной машине. Если на винчестере компьютера нет раз-

делов FAT или FAT32, то в качестве временной меры можно подключить дополнительный винчестер с разделом FAT32, чтобы сохранить большой объем информации при копировании из сети. Интерес может представлять и то, что с этой дискеты можно загрузить виртуальный компьютер!

Использование ресурсов компьютеров сети и расширение возможностей рабочей станции

Самые интересные изобретения и открытия делались на стыке различных областей технических знаний. Весьма заманчивые возможности открываются перед пользователями персональных компьютеров, если попытаться применить сетевые технологии для работы в локальном режиме. Анализируя практику работы в сети, я обнаружил, что значительная часть работ не требует наличия настоящей сети. Часто сеть позволяет лишь усилить вычислительные возможности рабочей станции. Почему бы не применить некие сетевые технологии для работы на локальном компьютере, который включен в локальную сеть, но может работать самостоятельно. Компьютер в этом случае должен быть не совсем обычный. Скорее это два компьютера, собранные в одно целое. Многие пользователи персональных компьютеров обновляют свою технику. При этом старые компьютеры, оставаясь вполне работоспособными, оказываются не у дел. Тем не менее есть возможность применить эти машины с большой пользой. Более того, польза оказывается такой существенной, что, вполне вероятно, кто-то решит применить для этих целей не старый, а вполне современный компьютер.

Для создания модернизированной рабочей станции потребуются два компьютера. Один — обычная рабочая станция, другой — вспомогательный компьютер, который может не иметь монитора, клавиатуры и мыши (к сожалению, не все материнские платы допускают такую работу). С внешним миром этот компьютер связан двумя кабелями. Витая пара соединяет его с современным компьютером, а кабель RS232 — с модемом. С точки зрения постороннего человека, это просто отдельно стоящий корпус. Для идентификации ролей присвоим компьютерам имена. Компьютер с монитором назовем PIU (The processor with the interface of the user, процессор с интерфейсом пользователя), а отдельно стоящий компьютер назовем APEC (The auxiliary processor for external connections, вспомогательный процессор для внешних подключений). Реально функциональное назначение этих компьютеров, конечно, шире, чем указано в кратком имени. Конструктивно компьютеры могут быть как отдельными устройствами, так и собранными в одном корпусе. В отдельных случаях могут потребоваться дополнительные устройства.

Области применения устройства (или комплекса устройств), о котором рассказывается в этой главе, могут быть очень многообразны. Мы рассмотрим работу устройства в качестве обычной рабочей станции, обладающей необычными свойствами.

Практически каждому компьютеру приходится взаимодействовать с окружающей его техникой специального назначения (рис. 6.14). Это принтеры, сканеры, модемы, коммутаторы (хабы) и другие устройства. Каждое из таких устройств имеет свою программу (драйвер), обеспечивающую его работу в среде операционной системы, установленной на рабочей станции. Чем активнее используется компьютер, тем больше задач в один и тот же момент ему приходится решать.

Рис. 6.14. Рабочая станция и ее окружение

Думаю, что вам приходилось обращать внимание на то, как компьютер начинает "замедляться" во время выполнения тех или иных задач. А в процессе выполнения подключения к Интернету, во время вывода объемных материалов на печать, обмена большими массивами информации по сети работа на компьютере практически останавливается. А если еще постоянно включен антивирусный монитор... Не секрет, что значительная часть заражения вирусами происходит в момент временного отключения антивирусного монитора ввиду помех, которые он создает нормальной работе компьютера. Когда же

на этой машине еще пишется и отлаживается программный код, "задумчивость" компьютера может стать довольно раздражающим фактором. Можно наращивать вычислительную мощность рабочей станции, приобретая все более современное и производительное оборудование. Но при высокой цене такого суперсовременного компьютера окажется, что большую часть времени его ресурсы используются нерационально. При этом "устаревшая" техника будет пылиться вообще без дела. Но есть другой выход из создавшегося положения. Следует реально разделить процессы, идущие в компьютере, на непересекающиеся потоки. Один из вариантов такого разделения — запускать эти процессы в отдельном устройстве, временная перегрузка которого не приведет к торможению или остановке процессов, которые видны пользователю. Таким устройством может стать либо отдельный компьютер, либо дополнительная материнская плата, расположенная в одном корпусе с основной. На рис. 6.14 наше устройство изображено в виде сдвоенного системного блока, заключающего в себе компьютеры PIU и APEC.

Как всякий уважающий себя компьютер, PIU и APEC должны иметь каждый свою операционную систему. При этом совершенно не имеет значения, какая конкретно система работает на каждом из них. Выбор операционной системы зависит от множества факторов, которые в этой главе не рассматриваются. Единственно важное условие, определяющее выбор операционной системы, — она должна поддерживать работу в сети. Еще одно важное условие для APEC, — должна быть возможность работы компьютера без клавиатуры и монитора, т. е. в процессе загрузки компьютер не должен останавливаться, выдавая сообщение, что он не нашел монитор или клавиатуру. Для того чтобы проверить это, можно включить компьютер без монитора и клавиатуры, а затем, подождав, пока винчестер прекратит процедуры записи/чтения, осторожно подключить к видеоадаптеру выключенный монитор и включить его. Если на экране будет нормальный рабочий стол или приглашение ввести пароль, то условие выполняется. Если вам не повезло, и обязательно требуется подключение клавиатуры и монитора, то можно применить даже не совсем исправные устройства, чтобы дать возможность компьютеру загрузиться.

Соберем PIU и APEC в единый комплекс. Специальных стандартов или правил для объединения компьютеров нет, многое зависит от характера поставленных задач и технических возможностей. Как вариант, можно рекомендовать соединение двух машин с помощью сетевого кабеля и сетевых адаптеров. При этом, когда оба компьютера работают, связь между ними возможна именно по сети, процессы, идущие на них, практически не взаимодействуют между собой. Если сами операционные системы слабо подвержены зависанию (например, Windows 2000), то получившийся комплекс, кроме высокой надежности, будет обладать широкими возможностями по распределению задач между PIU и APEC.

Я предчувствую, что у вас созрел резонный вопрос: "Как же мы будем распределять задачи, если можем общаться только с одной машиной?"

С ответа на этот вопрос и начинается огромное поле для экспериментов, которое мной пройдено лишь с самого краю. В настоящее время существует несколько способов удаленного взаимодействия с рабочим столом компьютера. Испытаны и показали следующие прекрасные результаты:

- уже известная вам программа Radmin;
- сервер терминалов в составе Windows 2000 Server;
- удаленный доступ к рабочему столу в Windows XP.

Во всех трех случаях операционной системой на PIU может быть любая версия Windows, начиная с Windows 95. Для APEC — во втором и третьем случае выбор очевиден, а в первом случае — любая ОС Windows, начиная с Windows 95 OSR2. Во втором и третьем случае при достаточности ресурсов у APEC можно пользоваться одновременно более чем одним сеансом работы на APEC. Это позволяет решать некоторые специфические задачи, связанные с непрерывным контролем процессов или продолжительными вычислениями.

Надо сказать, что существуют программы и для межплатформенного взаимодействия компьютеров. В этом случае будет возможна работа вспомогательной машины под Linux, например. Но мы рассмотрим вариант, уже испытанный автором, исправно работающий на протяжении двух лет. Состав комплекса следующий:

- PIU — компьютер с процессором AMD, 500 МГц, 256 Мбайт оперативной памяти, HDD — 40 Гбайт. Операционные системы — Windows 98 SE и Windows XP, основное программное обеспечение — Office 2000 Pro, пакет программ для работы с графикой, среда разработки программ;
- APEC — компьютер с процессором P-200, 64 Мбайт оперативной памяти, HDD — 20 Гбайт. Операционная система Windows 2000 Pro. К этому компьютеру подключен внешний модем и принтер.

Оба компьютера снабжены сетевыми адаптерами.

Для обеспечения возможности бесперебойной работы, независимо от сетевого подключения к серверу, компьютерам присвоены фиксированные IP-адреса.

На оба компьютера установлена программа Radmin, причем для APEC — в режиме сервиса (запускается при загрузке операционной системы).

На APEC, кроме того, установлены программы: прокси-сервер, почтовый сервер, Web-сервер, FTP-сервер, сервер точного времени, антивирусная программа.

Монитор и клавиатура подключались к APEC только в процессе начальной установки системы и программы Radmin. В дальнейшем для уменьшения нагрузки на систему программно был отключен видеоадаптер.

Для обеспечения удобного подключения к локальной сети использовался концентратор, через который осуществляется связь между компьютерами, но при отсутствии сети компьютеры можно соединить с помощью перекрестного кабеля. Если сетевые карты имеют BNS-разъемы, то возможно соединение и коротким коаксиальным кабелем.

Задачи, решаемые компьютерами PIU и APEC

Понятно, что PIU используется, как и большинство рабочих станций, для решения ежедневных задач. Специфика моей работы заключается в частом обращении ко мне сотрудников, при этом необходимо оперативно запустить какую-либо программу, отредактировать или создать документ, получить отчет из базы данных, на создание которого может быть затрачено несколько минут, тогда как основная задача, выполняемая на этом компьютере — разработка приложения — не должна останавливаться.

Связь с Интернетом у нас обеспечивается по обычной телефонной линии (dial-up), причем качество линии оставляет желать лучшего (я думаю, что в этом я не одинок). Процедура отправки/получения почты может занимать несколько десятков минут. Раньше в такие моменты никаких других действий на компьютере не допускалось, случайный сбой мог привести к обрыву соединения, да и само выполнение других задач в это время осложнено высокой загрузкой процессора. Теперь задачи по отправке и получению почты взял на себя APEC. На PIU эта процедура занимает всего пару секунд, а дальше почтовый сервер сам регулярно по расписанию или при получении очередного сообщения для отправки дозванивается до провайдера, отправляет и получает почту. При этом на PIU можно спокойно продолжать работу. Бывает, что во время подключения к Интернету ресурсы компьютера расходуются настолько активно, что работа с другими приложениями в это время невозможна. Снова спасает APEC. Пока идет установка связи, можно спокойно работать. Как только связь установилась, можно подключаться к любому ресурсу Интернета через прокси-сервер на APEC. Причем, если комплекс включен в сеть, в одно и то же время в Интернет может входить несколько человек.

Работа на компьютере всегда сопряжена с риском потери данных. Для уменьшения этого риска следует регулярно сохранять копии рабочих документов. Этим тоже занимается APEC в автоматическом режиме.

Часть задач по обработке данных, которые мне приходится выполнять, занимает весьма продолжительное время. Причем никаких действий от оператора не требуется, остается только ждать. Переложив подобные задачи на процессор и память APEC, можно продолжать работать, не теряя времени на ожидание.

Кроме того, время от времени на APEC происходит синхронизация с часами на сервере точного времени в Интернете. Мы все уже привыкли к тому, что на нашем комплексе всегда точное время. Как это ни странно, раньше время могло отличаться от точного на десятки минут. Проверьте время на своем компьютере. Если вы не обращали на него внимания специально, то результат может вас удивить.

Добавим ко всему, что на APEC работает антивирусный монитор, не отнимающий ресурсов у PIU.

Общение с APEC может происходить двумя путями. Первый путь — обычные сетевые папки. Второй путь — полный контроль через Radmin. При этом на рабочем столе PIU можно держать миниатюрное изображение рабочего стола APEC. Если необходимо, его легко развернуть на весь экран. Практически, работая с таким комплексом, трудно представить себе, что используются два компьютера. Работает один комплекс, решая общие задачи, но наличие двух процессоров и двух материнских плат позволяет решать эти задачи согласованно и без неприятных задержек и "зависаний".

Представляет интерес и то, что разрабатывать и "обкатывать" сетевые приложения (если программирование входит в круг ваших интересов и задач) можно на локальном рабочем месте. Если на APEC установить вторую сетевую плату и настроить маршрутизацию, то можно включать этот комплекс в любую сеть, не перестраивая внутренних связей. При этом PIU может быть защищен от неблагоприятных вторжений из сети существенно лучше, чем при прямом включении через концентратор.

Пользуясь описанием, настроить Radmin для работы с двумя компьютерами несложно. Но применяя на APEC Windows XP, вы встретитесь с существенной проблемой: если на экране APEC (невидимом для вас) не выведено приглашение Windows XP или не осуществлен вход в сеанс пользователя, то Radmin не сработает. В это время на экране компьютера находится список пользователей, и Radmin-server не загружен, причем наблюдается это, когда APEC не включен в домен и используется возможность быстрого переключения между пользователями. Но мы как раз и говорили о работе в локальном режиме, где нет никаких доменов. Для того чтобы вы имели возможность продолжить эксперименты с PIU и APEC, опишем процедуру подключения к компьютеру под управлением операционной системы Windows XP с помощью программы доступа к удаленному рабочему столу. В справочной сис-

теме Windows XP этот вопрос освещен несколько запутанно даже для имеющих опыт работы с сервером терминалов в системе Windows 2000 Server, поэтому пройдем пошагово весь путь настройки доступа к удаленному рабочему столу.

Для проведения описываемых настроек требуется обычный доступ к компьютеру в локальном режиме с его консоли (монитор, клавиатура, мышь), а также необходимо быть администратором компьютера. Если предполагается использование комплекса несколькими пользователями, то всех их надо сделать членами группы **Пользователи удаленного рабочего стола** (Remote Desktop Users). Компьютер PIU может иметь любую операционную систему семейства Windows, начиная с Windows 95.

Описание настроек APEC

Начнем с настройки APEC, для чего выполним следующие действия:

1. На панели управления откройте компонент **Установка и удаление программ**.
2. Нажмите кнопку **Установка компонентов Windows**.
3. Выберите компонент **Internet Information Services (IIS)** и нажмите кнопку **Состав**.
4. В списке **Internet Information Services — состав** выберите элемент **World Wide Web Service** (Служба WWW) и нажмите кнопку **Состав**.
5. В списке **Служба WWW — состав** установите флажок **Remote Desktop Web Connection** (Интернет-подключение к удаленному рабочему столу) и затем нажмите кнопку **ОК** (рис. 6.15).

В окне Мастера компонентов Windows нажмите кнопку **Далее**.

Откройте диспетчер служб Интернета. Для этого в **Панели управления** дважды щелкните на значке **Администрирование** и выберите **Internet Information Services** (Диспетчер служб Интернета). Появится окно, показанное на рис. 6.16.

Разверните структуру папок до папки имя_локального_компьютера\Веб-узлы\Веб-узел по умолчанию\tsweb.

Щелкните на значке папки **tsweb** правой кнопкой мыши и выберите команду **Свойства**.

Выберите вкладку **Безопасность каталога** в диалоговом окне **Свойства** (рис. 6.17).

В группе **Анонимный доступ и проверка подлинности** нажмите кнопку **Изменить**.

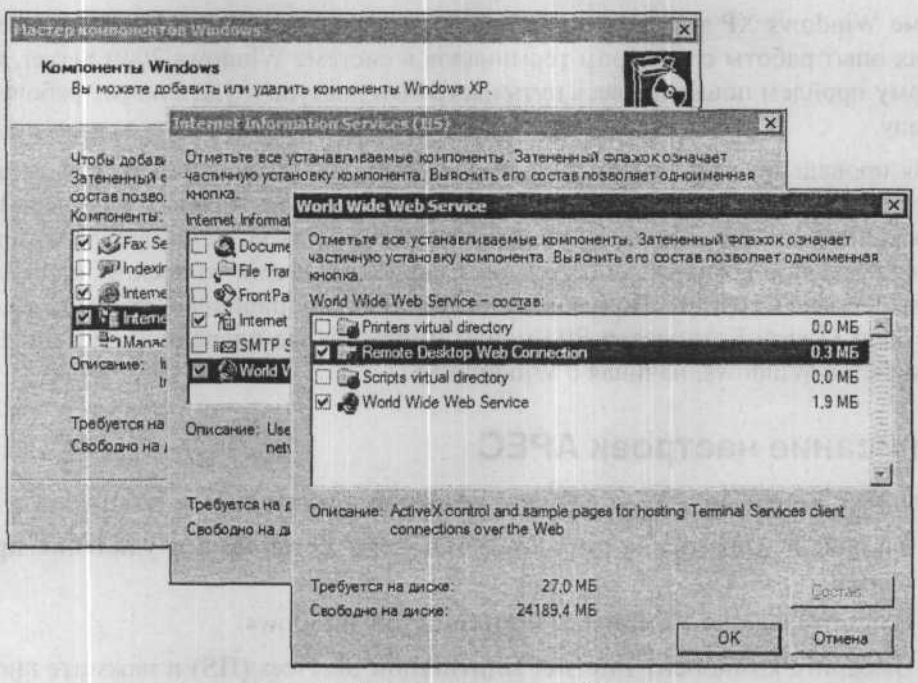

Рис. 6.15. Установка компонентов Windows

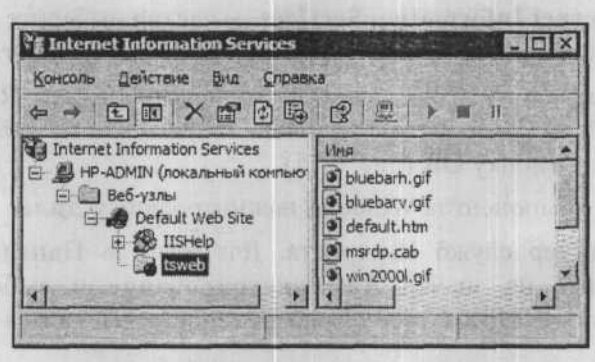

Рис. 6.16. Диспетчер служб Интернета

В диалоговом окне **Методы проверки подлинности** (рис. 6.18) установите флажок **Анонимный доступ** и дважды щелкните на кнопке **ОК**.

Щелкните на значке **Система** в **Панели управления**.

На вкладке **Удаленное использование** (рис. 6.19) установите флажок **Разрешить удаленный доступ к этому компьютеру** и нажмите кнопку **ОК**.

В области **Дистанционное управление рабочим столом** нажмите кнопку **Выбрать удаленных пользователей**.

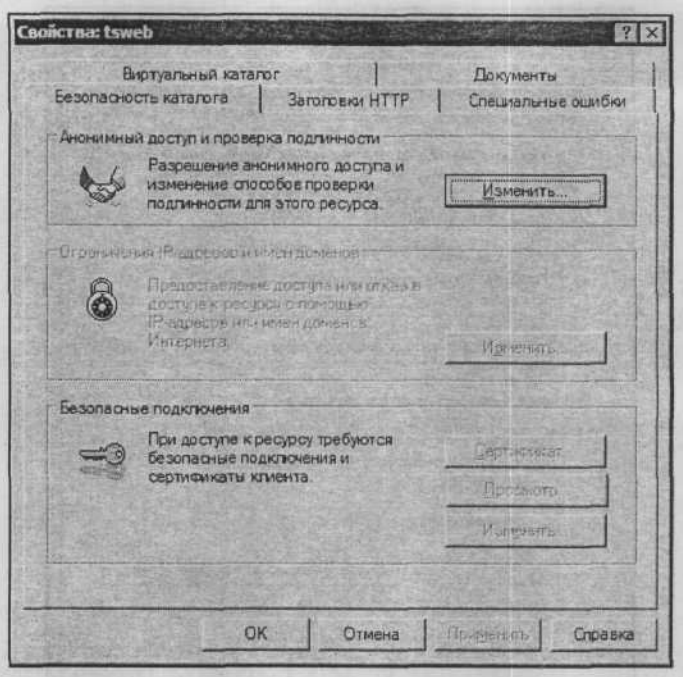

Рис. 6.17. Свойства каталога tsweb

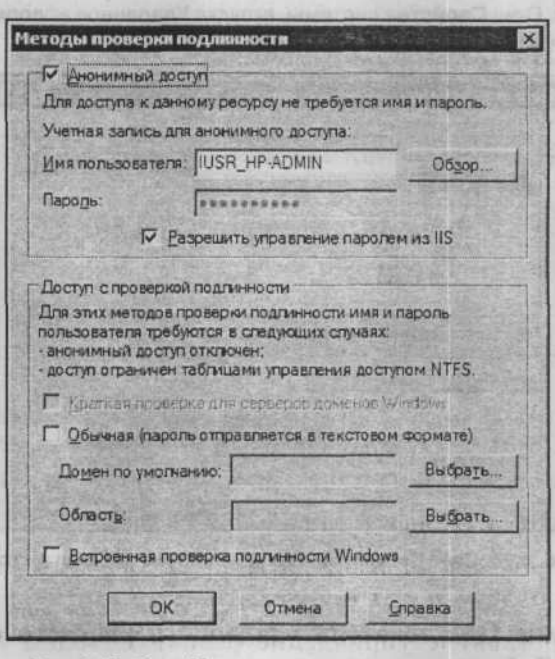

Рис. 6.18. Окно **Методы проверки подлинности**

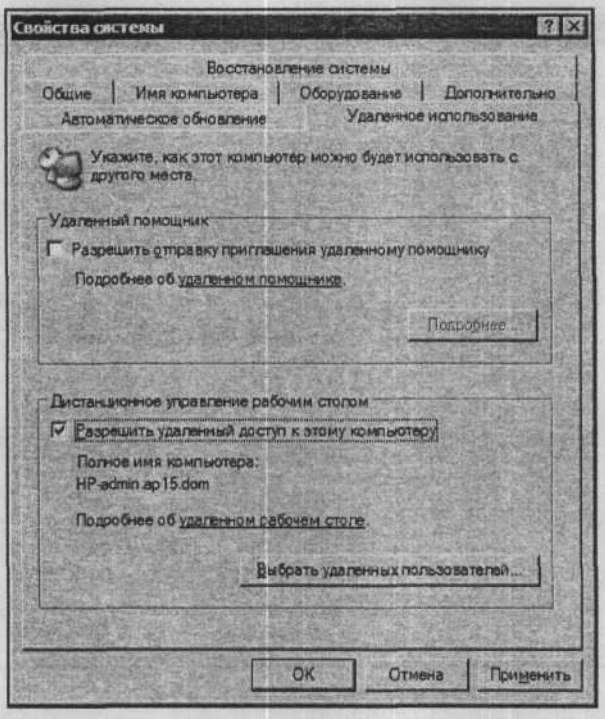

Рис. 6.19. Окно **Свойства системы**, вкладка **Удаленное использование**

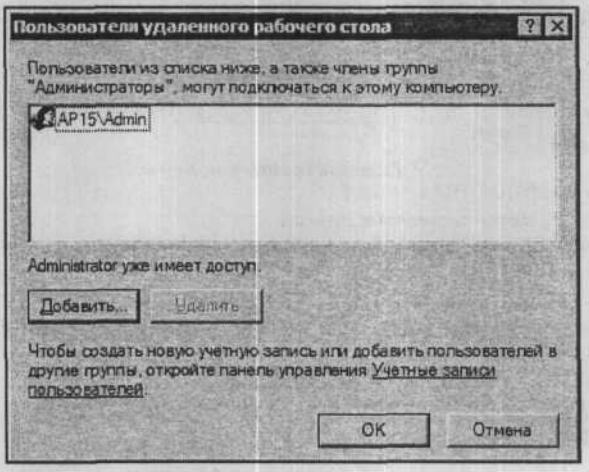

Рис. 6.20. Окно **Пользователи удаленного рабочего стола**

В диалоговом окне **Пользователи удаленного рабочего стола** (рис. 6.20) нажмите кнопку **Добавить**.

Примечание

Если единственным пользователем этого компьютера будет его администратор, то добавление пользователей не требуется.

В диалоговом окне **Выбор: Пользователи** (рис. 6.21) нажмите кнопку **Размещение**, чтобы задать область поиска.

Нажмите кнопку **Размещение**, чтобы указать размещение (если нет сетевых пользователей, то только локальные учетные записи).

Нажмите кнопку **Типы объектов**, чтобы обозначить типы объектов, поиск которых требуется выполнить (имеется в виду — группы или отдельные пользователи).

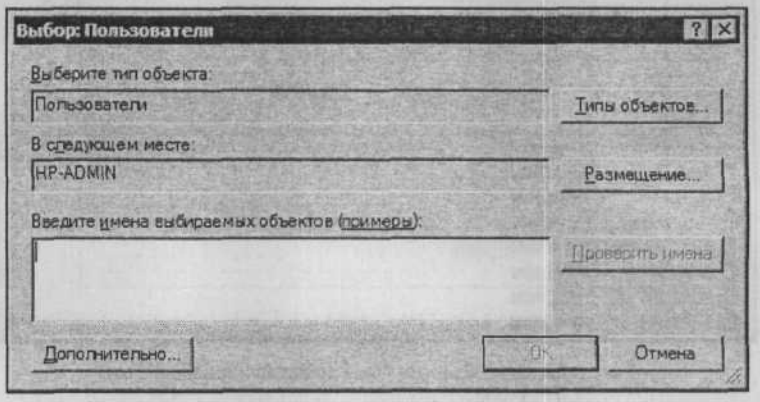

Рис. 6.21. Окно **Выбор: Пользователи** (свернуто)

В поле **Введите имена выбираемых объектов (примеры)** введите имена искомых объектов.

Нажмите кнопку **Проверить имена**.

Найдя имя, нажмите кнопку **ОК**. Теперь имя появится в списке пользователей в диалоговом окне **Пользователи удаленного рабочего стола**.

Убедитесь в наличии необходимых разрешений на удаленное подключение к данному компьютеру и нажмите кнопку **ОК**.

Окно **Выбор: Пользователи** может выводиться в двух видах: свернутом (рис. 6.21) и развернутом (рис. 6.22). Окно разворачивается при нажатии на кнопку **Дополнительно**. В развернутом виде учетные записи пользователей можно искать и выбирать из списка, прокручивая его, а также появляется возможность поиска пользователей по начальным символам имени учетной записи (при нажатии на кнопку **Поиск**).

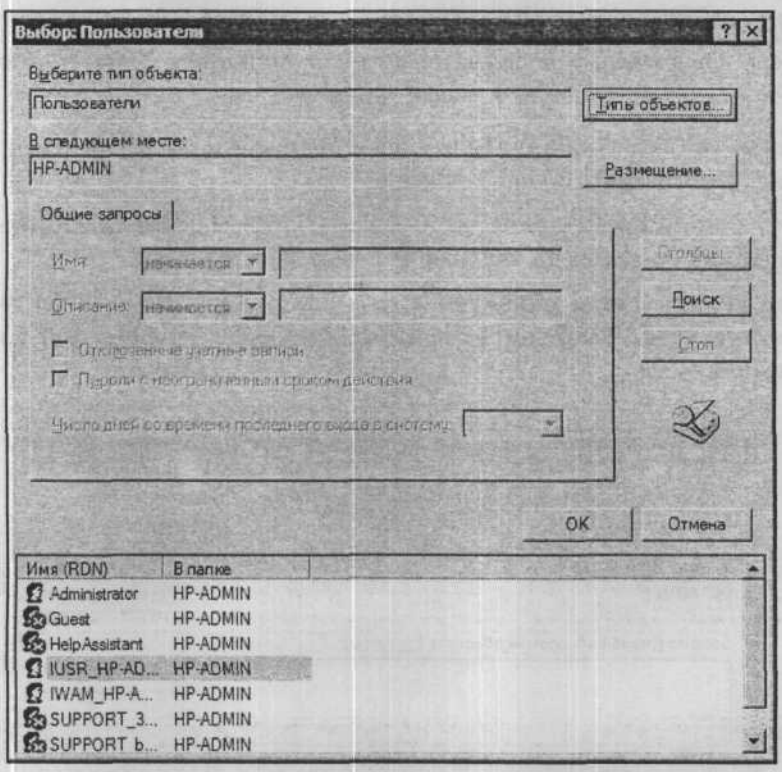

Рис. 6.22. Окно **Выбор: Пользователи** (развернуто)

Описание настроек для PIU

Выполнение описанных далее процедур требуется не всегда. На одной из машин с Windows 98 оказалось достаточным ввести в строку адреса в браузере адрес машины для подключения, после чего необходимые компоненты автоматически установились с подключаемой машины. Но в справочной системе Windows такая процедура не описана, поэтому будем придерживаться рекомендуемой методики.

Итак, выполним следующие действия:

1. На компьютере PIU, на котором установлена операционная система Windows 95, Windows 98, Windows NT 4.0 или Windows 2000, вставьте в дисковод установочный компакт-диск Windows XP Professional.
2. При появлении на экране страницы приветствия выберите ссылку **Выполнение иных задач**, а затем выберите вариант **Установка удаленного управления рабочим столом**.
3. Следуйте инструкциям на экране.

Установка подключения к рабочему столу компьютера APEC

Для подключения к Рабочему столу компьютера APEC необходимо сделать следующее:

1. Убедитесь, что выполнены все необходимые настройки компьютера APEC.
2. Убедитесь, что PIU имеет активное подключение к APEC или оба компьютера подключены к локальной сети.

> ***Примечание***
>
> Справочная система Windows XP говорит о необходимости применения в сети какого-либо метода определения имен, но это не обязательно, даже невозможно при локальной работе. Единственным неудобством в этом случае будет необходимость использования числового IP-адреса компьютеров вместо символьного.

3. На компьютере PIU запустите программу Microsoft Internet Explorer.
4. В поле **Адрес** введите IP-адрес каталога tsweb компьютера APEC (адрес задается в виде строки `http://192.168.115.90/tsweb`) и нажмите клавишу <Enter>. На экран будет выведена страница **Интернет-подключение к удаленному рабочему столу** (рис. 6.23).

> ***Примечание***
>
> Разумеется, что конкретное значение IP-адреса должно соответствовать адресу вашего компьютера APEC. Адрес страницы можно сохранить в папке **Избранное** для ускорения доступа к ней впоследствии.

5. В поле **Сервер** опять введите IP-адрес компьютера APEC.
6. При необходимости укажите размер экрана в поле **Размер** и поставьте флажок **Отправить учетные данные для данного подключения**.
7. Нажмите кнопку **Подключить**.

> ***Примечание***
>
> Для работы с программой **Интернет-подключение к удаленному рабочему столу** необходимо наличие Internet Explorer 4.0 или более поздней версии. Сама программа **Интернет-подключение к удаленному рабочему столу** может быть установлена на одном из доступных в сети компьютеров, например, на сервере, с которым обеспечена связь удаленных рабочих столов.

Для подключения можно применять и программу **Подключение к удаленному рабочему столу**, которая является усовершенствованным аналогом Клиента служб терминалов для Windows 2000 Server и может применяться вместо него.

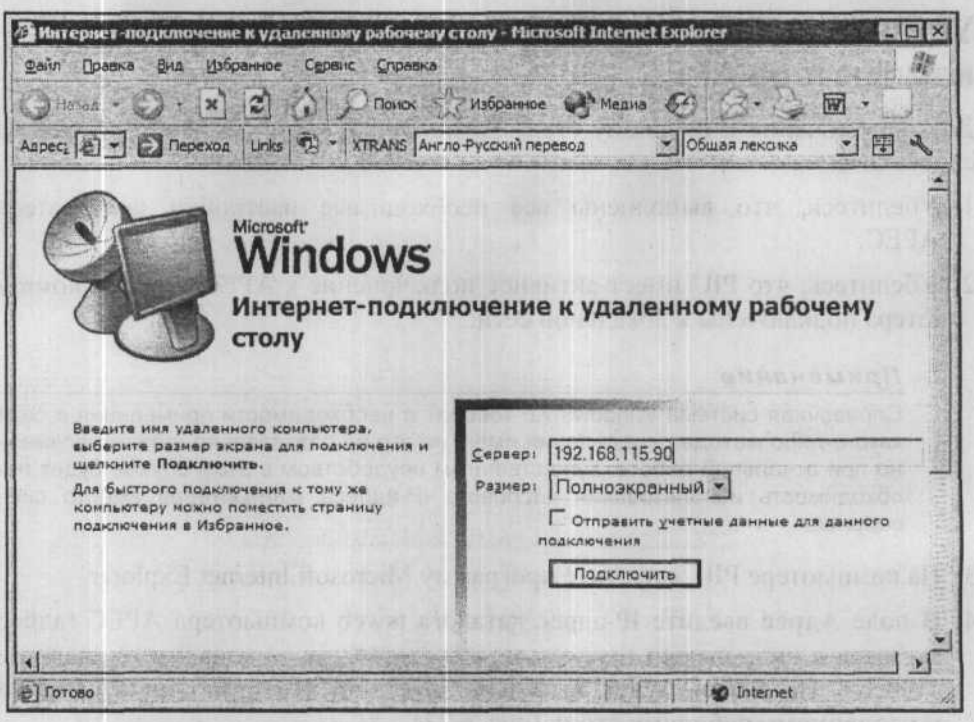

Рис. 6.23. Окно **Интернет-подключение к удаленному рабочему столу**

Опишем работу с программой **Подключение к удаленному рабочему столу**:

1. Для запуска данной программы нажмите кнопку **Пуск**, перейдите к пункту **Программы** или **Все программы**, **Стандартные**, **Связь** и выберите программу **Подключение к удаленному рабочему столу**. Появится окно, показанное на рис. 6.24. Для изменения параметров подключения (таких как размер экрана, сведения для автоматического входа и параметры производительности) перед подключением нажмите кнопку **Параметры** (рис. 6.26). Пролистав вкладки, можно настроить параметры отображения и управления удаленным рабочим столом. Для ускорения доступа впоследствии на вкладке **Общие** нажмите кнопку **Сохранить как**, введите имя файла параметров подключения и нажмите кнопку **Сохранить**. В поле **Компьютер** введите имя компьютера APEC (если в сети работает служба определения имен) или его IP-адрес.
2. Нажмите кнопку **Подключить**.

   Открывается диалоговое окно **Вход в Windows** в окне **Удаленный рабочий стол** (рис. 6.25).
3. В диалоговом окне **Вход в Windows** введите имя пользователя, пароль и домен (если требуется), а затем нажмите кнопку **OK**.

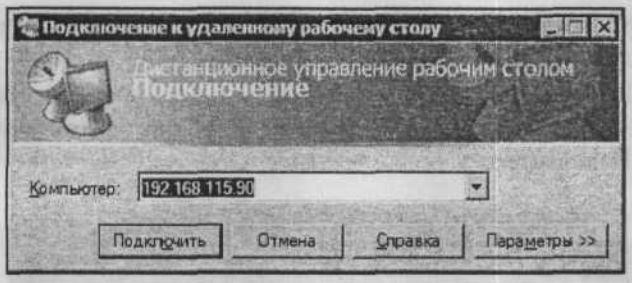

Рис. 6.24. Окно **Подключение к удаленному рабочему столу**

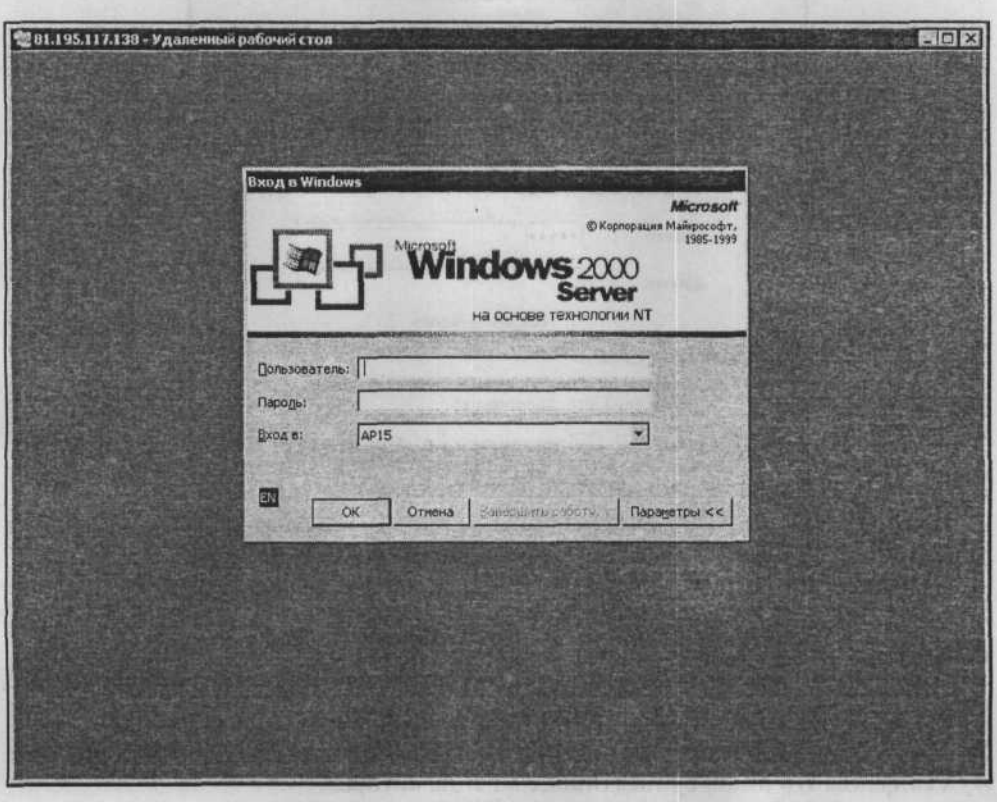

Рис. 6.25. Окно **Вход в Windows** (в окне **Удаленный рабочий стол**)

Подключения сохраняются в файлах удаленного рабочего стола (с расширением rdp). Файл типа rdp содержит все сведения о подключении к серверу терминалов, включая параметры, введенные на вкладке **Параметры** при сохранении файла. Пользователь имеет возможность создать любое количество файлов rdp, в том числе файлы подключения к одному и тому же серверу с разными настройками. Например, имеется возможность сохранить файл под-

ключения в полноэкранном режиме и файл подключения с размером экрана 800×600. Файлы rdp по умолчанию сохраняются как скрытые в папке **Мои документы**. Для редактирования файла rdp и изменения содержащихся в нем параметров подключения щелкните на имени файла правой кнопкой и выберите команду **Изменить**.

Рис. 6.26. Окно **Подключение к удаленному рабочему столу** с развернутыми вкладками параметров

Таким образом, вы имеете два способа подключения к рабочему столу APEC. Для систем с Windows 9*x* предпочтительней вариант с браузером, для Windows XP — вариант с программой **Подключение к удаленному рабочему столу**. Но это лишь субъективное мнение автора.

При подключении к удаленному рабочему столу машины, включенной в доменную сеть (зарегистрированную на сервере и настроенную для работы в сети), текущий сеанс пользователя блокируется. Если компьютер имеет локальный режим работы, но физически включен в сеть (аналог работы в Интернете), то текущий сеанс становится неактивным, а все запущенные программы продолжают работать. Пользуясь этим свойством, вы можете подключаться к рабочему столу APEC под разными именами и запускать не

связанные друг с другом программы, причем без риска случайного закрытия одной из них.

Примечание

Представляет интерес такой факт: работая с удаленным рабочим столом, нет необходимости входить в сеть, вы можете работать в сеансе локального пользователя. Следовательно, работать с комплексом можно в локальном режиме без настоящей сети.

При завершении работы с удаленным рабочим столом PIU (рис. 6.27) вы получаете возможность выбора: можно закрыть сеанс работы с рабочим столом APEC, а можно просто отключиться от него. При этом все программы будут продолжать функционировать, тогда как вы имеете возможность независимо от них работать с рабочим столом PIU.

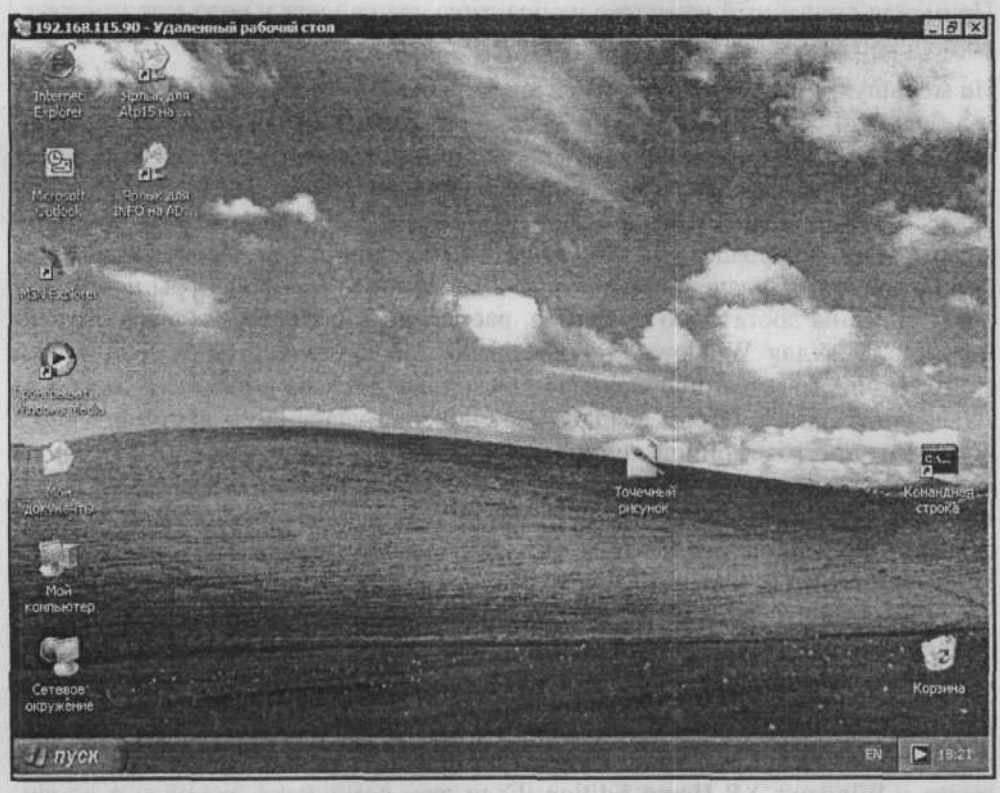

Рис. 6.27. Окно **Удаленный рабочий стол**

На настроенном комплексе многие задачи могут выполняться в фоновом режиме. Например, если компьютер APEC настроен на прием факсов, вам не придется отвлекаться от работы в момент получения сообщения или доку-

мента, но вы всегда можете просмотреть полученные материалы, открыв рабочий стол APEC. Даже если у APEC недостаточно ресурсов для комфортной работы при одновременном выполнении нескольких задач, вы не заметите этого. На экране PIU все будет происходить быстро. Если APEC на протяжении нескольких минут дозванивался до провайдера, затем несколько минут получал почту, вы сможете, запустив почтовый клиент на PIU, в доли секунды получить все сообщения, что были приняты на APEC. Аналогично, при отправке значительного объема информации по электронной почте вам не придется смотреть, как медленно происходит отправка и переживать по поводу прервавшейся связи, поскольку теперь все медленные процессы могут происходить незаметно для вас.

Разработчиков приложений клиент-сервер может заинтересовать возможность работы сразу с двумя частями приложения — серверной и клиентской.

Применяя описанный комплекс на практике, вы найдете у него еще множество положительных качеств.

Не меньшую пользу работа с удаленным рабочим столом способна принести и в большой сети, а также при работе через Интернет или телефонную сеть. Настраивая параметры доступа, можно минимизировать трафик и успешно работать при не слишком быстрой связи (модем). Некоторая медлительность связи будет компенсирована самой возможностью подключаться к своему компьютеру, находящемуся в десятках километрах от вас. Придется, правда, настроить сервер удаленного доступа. Для Windows 98 процедуры настройки были описаны достаточно подробно, рассмотрим настройку сервера удаленного доступа для Windows XP. В справочной системе этой операционной системы описывается подключение удаленного доступа к рабочему месту по телефонной линии. Чтобы создать подключение удаленного доступа к рабочему месту по телефонной линии, нажмите кнопку **Пуск**, выберите команды **Настройка** и **Панель управления**, затем дважды щелкните на значке **Сетевые подключения**. В группе **Типичные задачи** щелкните ссылку **Мастер сетевого подключения** и затем нажмите кнопку **Далее**. Выберите вариант **Подключить к сети на рабочем месте** и нажмите кнопку **Далее**. Установите переключатель в положение **Подключение удаленного доступа**, нажмите кнопку **Далее** и следуйте указаниям мастера нового подключения.

Удаленный доступ к компьютеру обеспечивается службой **Диспетчер автоподключений удаленного доступа**, которая включается по умолчанию на компьютерах Windows XP Professional, не являющихся членами доменов, а также в Windows XP Home Edition. Если ваш компьютер включен в домен, или **Диспетчер автоподключений удаленного доступа** отключен по другой причине, его нетрудно включить. Чтобы запустить **Диспетчер автоподключений удаленного доступа**, откройте последовательно **Панель управления | Администрирование | Управление компьютером | Службы**

и приложения | Службы, в правой панели окна **Управление компьютером** щелкните правой кнопкой мыши на службе **Диспетчер автоподключений удаленного доступа** и выберите команду **Запустить**. В столбце **Состояние** появится пометка **Работает**.

В среде Windows XP не будет работать программа ServerOK, с помощью которой можно было включать и выключать возможность удаленного доступа к компьютеру под управлением Windows 98 (адрес программы в Интернете — **http://serverok.da.ru/**). Но Windows XP позволяет управлять своими службами из командной строки. Для запуска и остановки службы **Диспетчер автоподключений удаленного доступа** достаточно в bat-файл включить команду `sc start RasAuto` или `sc stop RasAuto`. При этом, если ваш компьютер настроен и на прием факсов, а модем не может отличить попытку удаленного доступа от передачи факса, можно управлять и службой Fax, применив команды `sc start Fax` и `sc stop Fax`. Надо сказать, что в Windows XP практически все службы допускают управление из командной строки. Возможна автоматизация процессов вызова и приема вызова компьютером. Для включения вызова по телефону можно использовать команду rasdial с параметрами, которые есть в справке по данной команде. Команда rasdial, выполненная без параметров, показывает состояние текущих подключений.

Для работы с комплексом можно применить программы из следующего перечня:

1. Почтовый сервер Courier Mail Server (CMS 1.56). Адрес программы **http://courierms.narod.ru**.
2. Radmin (Remote administrator). Адрес программы **www.radmin.com**.
3. Простой Web-сервер AnalogX Simple Server. Адрес программы **www.analogx.com**.
4. Простой прокси-сервер AnalogX Proxy. Адрес программы **www.analogx.com**.
5. FTP-сервер TYPSoft FTP Server. Адрес программы **www.typsoft.com**. При необходимости можно прочитать описание версии 1.08 на русском языке по адресу **www.kadet.ru**.

Все программы (кроме Remote administrator, которая без регистрации может работать 40 дней) бесплатны, совместимы с любой операционной системой семейства Windows и опробованы автором в действии.

В описанном тандеме компьютеров допускается применять виртуальный компьютер, который сможет выполнять функции, не совместимые с теми, что выполняются на реальном компьютере. Если у реальной машины достаточно ресурсов, то в виртуальном виде могут работать дополнительные серверы сети, которые в дальнейшем, при наличии средств, можно "переселить" на

реальные компьютеры. То есть, это отличный полигон для экспериментов в сети.

Как уже отмечалось ранее, проводя любые настройки на сервере, необходимо документировать все изменения. Увлекшись экспериментом, желая добиться результата как можно быстрее, вы можете "заблудиться" в параметрах и свойствах. Обнаружив после неудачного эксперимента, что в сети что-то перестало работать, вам придется очень долго искать причины проблемы, если не документирован весь путь ваших экспериментов. Ваши записи, как клубок в сказках, покажут вам выход из незнакомого "леса".

Проводя эксперименты аккуратно, вы найдете для своей сети множество полезных и простых средств, помогающих решать задачи, которые, на первый взгляд, требуют значительных затрат для своей реализации.

ПРИЛОЖЕНИЕ

Справочные сведения

Работая в локальной сети, выходя в Интернет, настраивая маршрутизацию и другие сервисы сети, вы постоянно будете иметь дело с IP-адресами, масками подсети. Если не в обычном режиме работы сети, то во время экспериментов в ней вы можете столкнуться с конфликтами IP-адресов. Работа служб DHCP и WINS, а также DNS-серверов помогает организовать адреса сети и привязать к понятным именам. Но сами IP-адреса не могут быть произвольно назначены компьютерам или другим устройствам, работающим в сети. Для уверенной ориентации в пространстве IP-адресов необходимо знать диапазоны, на которые разбиты IP-адреса, а также область применения того или иного диапазона. Кроме собственно адреса, применяется такое свойство IP-адреса, как маска подсети. Работать с этой характеристикой будет намного легче, если вникнуть в ее суть. Но для этого придется применить двоичную и шестнадцатеричную системы счисления. Материалы, приведенные далее, помогут вам в освоении работы с IP-адресами.

Протоколы TCP/IP

Протоколы TCP/IP отвечают за передачу информации, проходящей по сети, и дальнейший ее прием. Протокол TCP делит всю информацию, подлежащую передаче, на отдельные блоки — пакеты. Протокол IP эти пакеты нумерует и посылает по заранее определенному цифровому адресу в виде кадра информации — пакета, в который вложен пакет, созданный по протоколу TCP. На приемном конце процедура выполняется в обратном порядке. Пакеты принимаются, сортируются и собираются в исходном сочетании. Цифровой, а вернее IP-адрес представляет собой четырехбайтную последовательность чисел, записываемых обычно в десятичном виде, например, так: 192.168.55.3. Сети условно делятся на классы, каждому из которых соответствует свой диапазон адресов (табл. П1).

Таблица П1. *Диапазоны адресов для классов сетей*

Класс сети	Маска подсети	Диапазон	Зарезервированные адреса
A	255.0.0.0	01.0.0.0 — 126.0.0.0	10.0.0.0 127.0.0.1
B	255.255.0.0	128.0.0.0 — 191.255.0.0	169.254.X.X С 172.16.0.0 по 172.31.0.0
C	255.255.255.0	192.0.0.0 — 222.0.0.0	С 192.168.0.0 по 192.168.255.0
D	255.0.0.0	224.0.0.0 — 239.255.255.255	
E	255.0.0.0	240.0.0.0 — 247.255.255.255	

Адрес 127.0.0.1 зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название loopback.

Маска подсети указывает на биты, предназначенные для обозначения адреса сети, в остальных позициях должен располагаться адрес компьютера. Приведены также применяемые диапазоны адресов для каждого класса, а также зарезервированные для особых случаев адреса, не применяемые в Интернете.

Структура адреса становится более понятной, если записать его в двоичном коде. Например, маска 255.255.255.0 в двоичном коде выглядит так: 11111111.11111111.11111111.0. Все позиции, предназначенные для записи адреса сети, заняты единицами. Адрес 198.168.55.1 выглядит как: 11000110.10101000.110111.1. По таблице можно определить, что это адрес сети класса "С", и адрес компьютера выражен единицей. Чем выше класс сети, тем больше может существовать адресов сети и тем меньше компьютеров может находиться в такой сети. Так, в классе А может быть 126 сетей, в каждой из которых — 254×254×254 компьютеров, а в классе С — 30×254×254 сетей, в каждой из которых 254 компьютера. Этот расчет очень приблизительный, поскольку не учитывает выделения групп адресов внутри диапазонов. Каждый компьютер в сети имеет свой уникальный адрес, назначенный администратором или полученный автоматически. Именно такие адреса воспринимает протокол IP.

Даже в самой сложной сети, допускающей передачу информации по наиболее короткому или наименее загруженному в настоящий момент пути, пакеты на приемном конце сортируются в последовательности их передачи, в то время

как реальная последовательность приема может существенно отличаться от исходной. Тем не менее искажений информации не происходит.

Описание расширений масок подсети

В отдельных случаях бывает удобно использовать значение маски подсети с расширением. Это позволяет логически разделить сети одного класса, а максимальное значение адреса сети в двоичном коде представлено непрерывным рядом единиц. Само расширение — это число двоичных единиц в значении маски подсети (табл. П2). Диапазон адресов, применяемый для локальных сетей с выходом в Интернет: с 192.168.0.0 по 192.168.255.0. Запись 192.168.0/24 показывает сеть с адресами 192.168.0.x с двумястами пятьюдесятью четырьмя возможными адресами узлов, запись — 192.168.0/25 говорит о подсети с 127 узлами, как и запись 192.168.128/25. При этом запись адреса сегмента сети —192.168.0/16 говорит о сети, которая может содержать 64 516 узлов. Для общего применения такие значения адресов не рекомендованы, но в закрытых сетях их можно использовать, как и адреса 10.0.0/24. Расширение, таким образом, позволяет более точно указать назначение адреса, независимо от принятых договоренностей о применении диапазонов адресов.

Таблица П2. *Расширение масок подсети от 24 до 32*

Маска подсети 255.255.255.0 /24 (11111111.11111111.11111111.00000000)			
1 подсеть			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.0	x.x.x.255		
Маска подсети 255.255.255.128 /25 (11111111.11111111.11111111.10000000)			
2 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.0	x.x.x.127	x.x.x.128	x.x.x.255
Маска подсети 255.255.255.192 /26 (11111111.11111111.11111111.11000000)			
4 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.0	x.x.x.63	x.x.x.128	x.x.x.191
x.x.x.64	x.x.x.127	x.x.x.192	x.x.x.255

Таблица П2 (продолжение)

Маска подсети 255.255.255.224 /27 (11111111.11111111.11111111.11100000)			
8 подсетей			
Наименьший IP	Наибольший IP	Наименьший IP	Наибольший IP
x.x.x.0	x.x.x.31	x.x.x.128	x.x.x.159
x.x.x.32	x.x.x.63	x.x.x.160	x.x.x.191
x.x.x.64	x.x.x.95	x.x.x.192	x.x.x.223
x.x.x.96	x.x.x.127	x.x.x.224	x.x.x.255
Маска подсети 255.255.255.240 /28 (11111111.11111111.11111111.11110000)			
16 подсетей			
Наименьший IP	Наибольший IP	Наименьший IP	Наибольший IP
x.x.x.0	x.x.x.15	x.x.x.128	x.x.x.143
x.x.x.16	x.x.x.31	x.x.x.144	x.x.x.159
x.x.x.32	x.x.x.47	x.x.x.160	x.x.x.175
x.x.x.48	x.x.x.63	x.x.x.176	x.x.x.191
x.x.x.64	x.x.x.79	x.x.x.192	x.x.x.207
x.x.x.80	x.x.x.95	x.x.x.208	x.x.x.223
x.x.x.96	x.x.x.111	x.x.x.224	x.x.x.239
x.x.x.112	x.x.x.127	x.x.x.240	x.x.x.255
Маска подсети 255.255.255.248 /29 (11111111.11111111.11111111.11111000)			
32 подсети			
Наименьший IP	Наибольший IP	Наименьший IP	Наибольший IP
x.x.x.0	x.x.x.7	x.x.x.128	x.x.x.135
x.x.x.8	x.x.x.15	x.x.x.136	x.x.x.143
x.x.x.16	x.x.x.23	x.x.x.144	x.x.x.151
x.x.x.24	x.x.x.31	x.x.x.152	x.x.x.159
x.x.x.32	x.x.x.39	x.x.x.160	x.x.x.167
x.x.x.40	x.x.x.47	x.x.x.168	x.x.x.175
x.x.x.48	x.x.x.55	x.x.x.176	x.x.x.183

Таблица П2 *(продолжение)*

Наименьший IP	Наибольший IP	Наименьший IP	Наибольший IP
x.x.x.56	x.x.x.63	x.x.x.184	x.x.x.191
x.x.x.64	x.x.x.71	x.x.x.192	x.x.x.199
x.x.x.72	x.x.x.79	x.x.x.200	x.x.x.207
x.x.x.80	x.x.x.87	x.x.x.208	x.x.x.215
x.x.x.88	x.x.x.95	x.x.x.216	x.x.x.223
x.x.x.96	x.x.x.103	x.x.x.224	x.x.x.231
x.x.x.104	x.x.x.111	x.x.x.232	x.x.x.239
x.x.x.112	x.x.x.119	x.x.x.240	x.x.x.247
x.x.x.120	x.x.x.127	x.x.x.248	x.x.x.255
Маска подсети 255.255.255.252 /30 (11111111.11111111.11111111.11111100)			
64 подсети			
Наименьший IP	**Наибольший IP**	**Наименьший IP**	**Наибольший IP**
x.x.x.0	x.x.x.3	x.x.x.128	x.x.x.131
x.x.x.4	x.x.x.7	x.x.x.132	x.x.x.135
x.x.x.8	x.x.x.11	x.x.x.136	x.x.x.139
x.x.x.12	x.x.x.15	x.x.x.140	x.x.x.143
x.x.x.16	x.x.x.19	x.x.x.144	x.x.x.147
x.x.x.20	x.x.x.23	x.x.x.148	x.x.x.151
x.x.x.24	x.x.x.27	x.x.x.152	x.x.x.155
x.x.x.28	x.x.x.31	x.x.x.156	x.x.x.159
x.x.x.32	x.x.x.35	x.x.x.160	x.x.x.163
x.x.x.36	x.x.x.39	x.x.x.164	x.x.x.167
x.x.x.40	x.x.x.43	x.x.x.168	x.x.x.171
x.x.x.44	x.x.x.47	x.x.x.172	x.x.x.175
x.x.x.48	x.x.x.51	x.x.x.176	x.x.x.179
x.x.x.52	x.x.x.55	x.x.x.180	x.x.x.183
x.x.x.56	x.x.x.59	x.x.x.184	x.x.x.187
x.x.x.60	x.x.x.63	x.x.x.188	x.x.x.191
x.x.x.64	x.x.x.67	x.x.x.192	x.x.x.195

Таблица П2 (окончание)

Наименьший IP	Наибольший IP	Наименьший IP	Наибольший IP
x.x.x.68	x.x.x.71	x.x.x.196	x.x.x.199
x.x.x.72	x.x.x.75	x.x.x.200	x.x.x.203
x.x.x.76	x.x.x.79	x.x.x.204	x.x.x.207
x.x.x.80	x.x.x.83	x.x.x.208	x.x.x.211
x.x.x.84	x.x.x.87	x.x.x.212	x.x.x.215
x.x.x.88	x.x.x.91	x.x.x.216	x.x.x.219
x.x.x.92	x.x.x.95	x.x.x.220	x.x.x.223
x.x.x.96	x.x.x.99	x.x.x.224	x.x.x.227
x.x.x.100	x.x.x.103	x.x.x.228	x.x.x.231
x.x.x.104	x.x.x.107	x.x.x.232	x.x.x.235
x.x.x.108	x.x.x.111	x.x.x.236	x.x.x.239
x.x.x.112	x.x.x.115	x.x.x.240	x.x.x.243
x.x.x.116	x.x.x.119	x.x.x.244	x.x.x.247
x.x.x.120	x.x.x.123	x.x.x.248	x.x.x.251
x.x.x.124	x.x.x.127	x.x.x.252	x.x.x.255

В табл. П3 показана связь между расширением маски подсети, двоичной записью маски и побайтовой записью для 32-разрядных адресов. В конце строки указано количество сетей и их класс, которые могут быть созданы с применением данной маски.

Таблица П3. *Связь между расширением маски подсети, двоичной записью маски и побайтовой записью*

Расш.	Маска подсети в двоичном представлении	Побайтовое представление	Кол.	Класс
/0	00000000.00000000.00000000.00000000	0.0.0.0	256	A
/1	10000000.00000000.00000000.00000000	128.0.0.0	128	A
/2	11000000.00000000.00000000.00000000	192.0.0.0	64	A
/3	11100000.00000000.00000000.00000000	224.0.0.0	32	A
/4	11110000.00000000.00000000.00000000	240.0.0.0	16	A
/5	11111000.00000000.00000000.00000000	248.0.0.0	8	A

Таблица П3 *(окончание)*

Расш.	Маска подсети в двоичном представлении	Побайтовое представление	Кол.	Класс
/6	11111100.00000000.00000000.00000000	252.0.0.0	4	A
/7	11111110.00000000.00000000.00000000	254.0.0.0	2	A
/8	11111111.00000000.00000000.00000000	255.0.0.0	1	A
/9	11111111.10000000.00000000.00000000	255.128.0.0	128	B
/10	11111111.11000000.00000000.00000000	255.192.0.0	64	B
/11	11111111.11100000.00000000.00000000	255.224.0.0	32	B
/12	11111111.11110000.00000000.00000000	255.240.0.0	16	B
/13	11111111.11111000.00000000.00000000	255.248.0.0	8	B
/14	11111111.11111100.00000000.00000000	255.252.0.0	4	B
/15	11111111.11111110.00000000.00000000	255.254.0.0	2	B
/16	11111111.11111111.00000000.00000000	255.255.0.0	1	B
/17	11111111.11111111.10000000.00000000	255.255.128.0	128	C
/18	11111111.11111111.11000000.00000000	255.255.192.0	64	C
/19	11111111.11111111.11100000.00000000	255.255.224.0	32	C
/20	11111111.11111111.11110000.00000000	255.255.240.0	16	C
/21	11111111.11111111.11111000.00000000	255.255.248.0	8	C
/22	11111111.11111111.11111100.00000000	255.255.252.0	4	C
/23	11111111.11111111.11111110.00000000	255.255.254.0	2	C
/24	11111111.11111111.11111111.00000000	255.255.255.0	1	C
/25	11111111.11111111.11111111.10000000	255.255.255.128		
/26	11111111.11111111.11111111.11000000	255.255.255.192		
/27	11111111.11111111.11111111.11100000	255.255.255.224		
/28	11111111.11111111.11111111.11110000	255.255.255.240		
/29	11111111.11111111.11111111.11111000	255.255.255.248		
/30	11111111.11111111.11111111.11111100	255.255.255.252		
/31	11111111.11111111.11111111.11111110	255.255.255.254		
/32	11111111.11111111.11111111.11111111	255.255.255.255		

Пример того, как преобразовать двоичное значение 11000000 в десятичное представление (192):

11000000 Bin = 128×1 + 64×1 + 32×0 + 16×0 + 8×0 + 4×0 + 2×0 + 1×0
= 128 + 64 + 0 + 0 + 0 + 0 + 0 + 0
= 128 + 64
= 192

Соответствие русских и английских наименований объектов системы

В зависимости от версии ОС, установленных пакетов обновлений, вариантов локализации, а также от некоторых других причин имена объектов, названия окон и меню могут встречаться и на русском, и на английском языке. В табл. П4 приведен список соответствия некоторых русских и английских наименований, которые могут быть приведены в окнах и меню по-английски, несмотря на то, что ОС русифицирована.

Таблица П4. *Соответствие некоторых английских и русских наименований элементов интерфейса*

Английское наименование	Русское наименование
Action	Действие
Active Directory	Служба каталогов Active Directory
Administration	Администрирование
Choice computer	Выбор компьютера
Common resources	Общие ресурсы
Computer Management	Управление компьютером
Domain	Домен (Область сети)
Internet Information Service	Службы Интернета
Local Security Setting	Локальные параметры безопасности
Open	Открыть
Start	Пуск
Subnet mask	Маска подсети
World Wide Web Service	Служба WWW

Обычно у начинающих администраторов возникают затруднения при поиске необходимой службы в окне **Службы** (Services). Число служб, которые перечислены в этом окне, может изменяться в зависимости от установленных компонентов системы и других программ. Наименования служб, как и самого окна, могут быть русскими или английскими. Для упрощения поиска необходимой службы в табл. П5 приведены соответствия русских и английских наименований. Некоторые службы не имеют русского имени, а другие наименования не всегда являются точным переводом английского варианта.

Таблица П5. *Английские и русские наименования служб*

	Наименование английское	**Наименование русское**
1	Alerter	Оповещатель
2	Application Layer Gateway Service	Служба шлюза уровня приложения
3	Application Management	Управление приложениями
4	Automatic Updates	Автоматическое обновление
5	Background Intelligent Transfer Service	Фоновая интеллектуальная служба передачи
6	ClipBook	Сервер папки обмена
7	COM+ Event System	Система событий COM+
8	COM+ System Application	Системное приложение COM+
9	Computer Browser	Обозреватель компьютеров
10	Cryptographic Services	Службы криптографии
11	DHCP Client	DHCP-клиент
12	Distributed Link Tracking Client	Клиент отслеживания изменившихся связей
13	Distributed Transaction Coordinator	Координатор распределенных транзакций
14	DNS Client	DNS-клиент
15	Error Reporting Service	Служба регистрации ошибок
16	Event Log	Журнал событий
17	Fast User Switching Compatibility	Совместимость быстрого переключения пользователей
18	Fax Service	Служба факсов
19	Help and Support	Справка и поддержка
20	Human Interface Device Access	Доступ к HID-устройствам

Таблица П5 (продолжение)

	Наименование английское	Наименование русское
21	IMAPI CD-Burning COM Service	Служба COM записи компакт-дисков IMAPI
22	Indexing Service	Служба индексирования
23	IPSEC Services	Службы IPSEC
24	Logical Disk Manager	Диспетчер логических дисков
25	Logical Disk Manager Administrative Service	Служба администрирования диспетчера логических дисков
26	Messenger	Служба сообщений
27	Net Logon	Сетевой вход в систему
28	NetMeeting Remote Desktop Sharing	NetMeeting Remote Desktop Sharing
29	Network Connections	Сетевые подключения
30	Network DDE	Служба сетевого DDE
31	Network DDE DSDM	Диспетчер сетевого DDE
32	Network Location Awareness (NLA)	Служба сетевого расположения (NLA)
33	NT LM Security Support Provider	Поставщик поддержки безопасности NT LM
34	Performance Logs and Alerts	Журналы и оповещения производительности
35	Plug and Play	Plug and Play
36	Portable Media Serial Number	Серийный номер переносного медиа-устройства
37	Print Spooler	Диспетчер очереди печати
38	Protected Storage	Защищенное хранилище
39	QoS RSVP	QoS RSVP
40	Remote Access Auto Connection Manager	Диспетчер автоподключений удаленного доступа
41	Remote Access Connection Manager	Диспетчер подключений удаленного доступа
42	Remote Desktop Help Session Manager	Диспетчер сеанса справки для удаленного рабочего стола
43	Remote Procedure Call (RPC)	Удаленный вызов процедур (RPC)
44	Remote Procedure Call (RPC) Locator	Локатор удаленного вызова процедур (RPC)

Таблица П5 (продолжение)

	Наименование английское	Наименование русское
45	Remote Registry Service	Удаленный реестр
46	Removable Storage	Съемные ЗУ
47	Routing and Remote Access	Маршрутизация и удаленный доступ
48	Secondary Logon	Вторичный вход в систему
49	Security Accounts Manager	Диспетчер учетных записей безопасности
50	Server	Сервер
51	Shell Hardware Detection	Определение оборудования оболочки
52	Smart Card	Смарт-карты
53	Smart Card Helper	Модуль поддержки смарт-карт
54	SSDP Discovery Service	Служба обнаружения SSDP
55	System Event Notification	Уведомление о системных событиях
56	System Restore Service	Служба восстановления системы
57	Task Scheduler	Планировщик заданий
58	TCP/IP NetBIOS Helper Service	Модуль поддержки NetBIOS через TCP/IP
59	Telephony	Телефония
60	Telnet	Telnet
61	Terminal Services	Службы терминалов
62	Themes	Темы
63	Uninterruptible Power Supply	Источник бесперебойного питания
64	Universal Plug and Play Device Host	Узел универсальных PnP-устройств
65	Upload Manager	Диспетчер отгрузки
66	Volume Shadow Copy	Теневое копирование тома
67	WebClient	Веб-клиент
68	Windows Audio	Windows Audio
69	Windows Firewall/Internet Connection Sharing	Брандмауэр Интернета (ICF) /Общий доступ к Интернету (ICS)
70	Windows Image Acquisition (WIA)	Служба загрузки изображений (WIA)
71	Windows Installer	Windows Installer
72	Windows Management Instrumentation	Инструментарий управления Windows

Таблица П5 (окончание)

	Наименование английское	Наименование русское
73	Windows Management Instrumentation Driver Extension	Расширения драйверов WMI
74	Windows Time	Служба времени Windows
75	Wireless Zero Configuration	Беспроводная настройка
76	WMI Performance Adapter	Адаптер производительности WMI
77	Workstation	Рабочая станция

Назначение службы приводится в окне **Службы**. Это описание тоже может быть на английском языке. Если это так, то вам придется перевести его самостоятельно или обратиться к другим документам, где приводится такой перевод.

Порты

Не менее важно понимать, что для работы программ или вирусов в сети необходимо не только иметь адрес назначения, но и порт, через который можно проникнуть в систему. Портами этими пользуются как TCP-протокол, так и UDP-протокол (User Datagram Protocol, пользовательский протокол данных), который достаточно часто используется приложениями для передачи данных. В Интернете можно найти большие списки портов, которые используются вирусами, например, по адресу **http://www.sans.org/resources/idfaq/oddports.php**.

Но, просматривая их, вы увидите, что лучше закрыть все лишние (не используемые приложениями) порты, чтобы защитить компьютер от атак из Интернета. Список наиболее распространенных портов, которые могут применяться различными известными приложениями, лучше знать если не наизусть, то "близко к тексту". Число портов, которые могут использоваться приложениями, очень велико — 65 336. Этого числа достаточно для того, чтобы у вашего компьютера всегда были свободные порты, необходимые для работы различных программ связи, например. Тем не менее есть определенный список портов, которые рекомендовано использовать для стандартных сервисов сети. Для таких сервисов отведены первые 1024 номера. Самые распространенные сервисы, такие как FTP, Telnet, SMTP, Time, DNS, TFTP, HTTP, POP3, NNTP обычно используют порты, номера которых приведены в табл. П6.

Таблица П6. *Наиболее распространенные номера портов*

Номер	Сервис	Протокол
20	FTP-data	TCP
21	FTP	TCP
23	Telnet	TCP
25	SMTP	TCP
37	Time	TCP
53	DNS	UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
119	NNTP	TCP

В некоторых случаях, когда рекомендуемый для работы программы порт по какой-либо причине применить нельзя, следует использовать и порты из приведенного списка, если нет программ, которые их используют. Например, создавая VPN, вы можете столкнуться с ситуацией, когда запланированный для применения порт закрыт на одном из серверов, через который должна осуществляться связь. В этом случае можно применить порт, предназначенный для работы стандартных сервисов, который наверняка открыт на всех серверах провайдеров Интернета.

www.bhv.ru

Поляк-Брагинский А. В.
Сеть своими руками, 2-е издание

Магазин "Новая техническая книга"

СПб., Измайловский пр., д. 29, тел. (812) 251-41-10

Отдел оптовых поставок

e-mail: opt@bhv.spb.su

Для тех, кто решил самостоятельно создать сеть у себя дома или в офисе, эта книга станет незаменимым помощником. В ней детально рассмотрены все вопросы организации и обслуживания локальных сетей: от выбора аппаратной части и монтажа сети до настройки операционной системы и последующего ее администрирования. Особенно обстоятельно изложены методы согласования в одной сети старых и новых компьютеров, работающих с разными операционными системами, а также организации удаленного доступа к сети и защиты от несанкционированных действий. Ссылки на ресурсы Интернета, подробные инструкции по настройке программного и аппаратного обеспечения помогут сэкономить время и средства при развертывании собственного ЛВС. Книга предназначена для квалифицированных пользователей и начинающих администраторов.

Поляк-Брагинский Александр Владимирович, начальник отдела компьютерного обеспечения, специалист в области организации и эксплуатации малых и средних локальных сетей, автор книги «Сеть под Windows» и ряда статей в журнале «Мир ПК».

www.bhv.ru

Поляк-Брагинский А. В.
Сеть под Microsoft Windows

Магазин "Новая техническая книга"
СПб., Измайловский пр., д. 29, тел. (812) 251-41-10

Отдел оптовых поставок
e-mail: opt@bhv.spb.su

Организация локальной сети своими руками

Как создать и настроить локальную сеть дома, в офисе, на предприятии? Что необходимо знать для обеспечения ее надежной и эффективной работы? Отвечает на все эти вопросы профессионал, имеющий большой опыт организации и эксплуатации малых и локальных сетей. Автор дает практические рекомендации по выбору и установке сетевого оборудования, подробные инструкции по настройке компьютеров и администрированию сетей, рассматривает наиболее типичные неполадки и способы их устранения. Многочисленные примеры помогут читателям самостоятельно освоить процедуры подключения и настройки компьютеров, принтеров и другого оборудования, познакомят с методами организации пользователей в группы и распределения их прав в сети, обучат приемам администрирования. В книге приводятся необходимые теоретические и справочные сведения, а также ссылки на интернет-ресурсы.

www.bhv.ru

Столлингс В.
Компьютерные сети, протоколы и технологии Интернета (+CD-ROM)

Магазин "Новая техническая книга"

СПб., Измайловский пр., д. 29, тел. (812) 251-41-10

Отдел оптовых поставок

e-mail: opt@bhv.spb.su

Компьютерные сети, протоколы и технологии Интернета — новейшая книга популярного автора Вильяма Столлингса, которая дает исчерпывающий и наглядный обзор вычислительных сетей и передовых интернет-технологий. Автор использует нисходящий подход в виде модульной схемы, который позволяет преподавателям и научным работникам проектировать курсы и планировать обучение, отвечающее их собственным потребностям.

Сопровождающие материалы Web-сайта позволяют преподователям использовать их непосредственно в своих курсах и помогают студентам и научным работникам при изучении проблем производительности в реальных проектах.

В книге дается современный обзор разработок протоколов и алгоритмов, основанных на Интернете.

Вильям Столлингс внес выдающийся вклад в технологию разработки вычислительных сетей и компьютерной архитектуры. Автор 18 книг, он шесть раз получил приз за лучший учебник года по компьютерным наукам и инженерии Ассоциации авторов учебников и академических изданий. В настоящее время является независимым консультантом, в число клиентов которого входят производители и пользователи программного обеспечения и крупнейшие государственные институты. В. Столлингс имеет степень доктора наук Массачусетского технологического института в области вычислительной техники.

www.bhv.ru

Стивен Дж. Бигелоу
Сети: поиск неисправностей, поддержка и восстановление

Магазин "Новая техническая книга"

СПб., Измайловский пр., д. 29, тел. (812) 251-41-10

Отдел оптовых поставок

e-mail: opt@bhv.spb.su

Решайте все свои маленькие и большие сетевые проблемы с помощью этой авторитетной и всеобъемлющей книги! В руководстве, написанном известным специалистом по устранению неисправностей Стивеном Бигелоу, рассмотрены архитектуры, протоколы, операционные системы, а также все особенности сетевого оборудования: кабелей, сетевых карт, накопителей, адаптеров, хабов, роутеров и многих других. Кроме изучения общих принципов поиска неисправностей и описания сотен специфических признаков неисправностей, вы также овладеете практическими приемами сетевого администрирования, резервирования и восстановления данных, обеспечения безопасности.

Стивен Дж. Бигелоу, опытный инженер-электронщик, основатель и президент фирмы Dynamic Learning Systems, специализирующейся в области обслуживания ПК, периферийного и сетевого оборудования. Автор нескольких бестселлеров из области компьютерной литературы, включая пять изданий «Troubleshooting, Maintaining & Reparing PCs», редактор журнала «The PC Toolbar Newsletter».

www.bhv.ru

Книги издательства "БХВ-Петербург" в продаже:

Магазин "Новая техническая книга": СПб., Измайловский пр., д. 29, тел. (812) 251-41-10
Отдел оптовых поставок: e-mail: opt@bhv.spb.su

Внесерийные книги

Mandrakesoft. Установка и использование Mandrakelinux 10.0 (+CD-ROM)	144 с.
Андрианов В., Соколов А. Автомобильные охранные системы. Справочное пособие	272 с.
Богданов-Катьков Н. Струйные принтеры для дома и офиса	224 с.
Боков В. Физика магнетиков. Учебное пособие для вузов	129 с.
Бутиков Е. Оптика: Учебное пособие для студентов физических специальностей вузов, 2-е изд.	480 с.
Быков А. и др. ADEM CAD/CAM/TDM. Черчение, модернизация, механообработка (+CD-ROM)	320 с.
Гасфилд Д. Строки, деревья и последовательности в алгоритмах	654 с.
Гласс Г., Эйблс К. Unix для программистов и пользователей, 3-е изд.	848 с.
Гольдштейн Б. Стек протоколов ОКС7. Подсистема ISUP. Справочник	480 с.
Гольдштейн Б. Интерфейсы V5.1 и V5.2. Справочник	288 с.
Гольдштейн Б. Системы коммутации, 2-е изд.	318 с.
Гольдштейн Б. Call-центры и компьютерная телефония	372 с.
Гурова А. Герои меча и магии. По мотивам одноименной компьютерной игры	320 с.
Дорот В., Новиков Ф. Толковый словарь современной компьютерной лексики, 3-е изд.	608 с.
Зыль С. QNX Momentics: основы применения (+CD-ROM)	256 с.
Зыль С. Операционная система реального времени QNX: от теории к практике, 2-е изд. (+CD-ROM)	192 с.
Иванов К. Сборник задач по элементарной математике для абитуриентов, 4-е изд.	352 с.
Канторович Л., Акилов Г. Функциональный анализ, 4-е изд.	816 с.
Карпюк В. MS Windows XP Professional. Опыт сдачи сертификационного экзамена 70-270	528 с.
Корнеев В., Киселев А. Современные микропроцессоры, 3-е изд.	448 с.
Кохась К. Задачи Санкт-Петербургской олимпиады школьников по математике 2003 года	224 с.
Кохась К. Задачи Санкт-Петербургской олимпиады школьников по математике 2004 года	224 с.
Культин Н. Visual Basic. Освой на примерах (+CD-ROM)	288 с.

Макаров Б. и др. Избранные задачи по вещественному анализу, 2-е изд.	624 с.
Малыхина М. Базы данных: основы, проектирование, использование	512 с.
Палмер М., Синклер Р. Проектирование и внедрение компьютерных сетей. Учебный курс., 2-е изд.	240 с.
Петров Ю. Новые главы теории управления и компьютерных вычислений	192 с.
Пирогов В. Ассемблер. Учебный курс. 2-е изд.	1056 с.
Пог Д. MS Windows XP Home Edition: недокументированные возможности	768 с.
Погорелов В. AutoCAD 2005 для начинающих	400 с.
Половко А. Интерполяция. Методы и компьютерные технологии их реализации	320 с.
Попов А. Администрирование Windows с помощью WMI и WMIC (+CD-ROM)	752 с.
Попов С. Аппаратные средства мультимедиа. Видеосистема PC	400 с.
Правин О. Правильный самоучитель работы на компьютере, 2-е изд.	496 с.
Прохоров А. Интернет: как это работает	280 с.
Роб П. Системы баз данных: проектирование, реализация и управление, 5-е изд.	299 с.
Роб П. Системы баз данных: проектирование, разработка и использование	1200 с.
Робачевский А. Операционная система UNIX	528 с.
Романовский И. Дискретный анализ, 3-е изд.	320 с.
Скляров Д. Искусство защиты и взлома информации	288 с.
Соколов А., Андрианов В. Альтернатива сотовой связи: транкинговые системы	448 с.
Соколов А., Степанюк О. Защита от компьютерного терроризма	126 с.
Соломенчук В., Соломенчук П. Железо ПК 2004	368 с.
Суворов К., Черемных М. Справочник Delphi. Базовые классы	576 с.
Титтел Э., Чеппел Л. TCP/IP. Учебный курс (+CD-ROM)	976 с.
Феличи Д. Типографика: шрифт, верстка, дизайн	360 с.
Фленов М. Библия Delphi (+CD-ROM)	880 с.
Фленов М. Программирование в Delphi глазами хакера (+CD-ROM)	368 с.
Фленов М. Программирование на C++ глазами хакера (+CD-ROM)	336 с.
Фрей Д. AutoCAD и AutoCAD LT для начинающих	680 с.
Частиков А. Архитекторы компьютерного мира	384 с.
Яцюк О. Основы графического дизайна на базе компьютерных технологий (+CD-ROM)	270 с.

www.bhv.ru

Книги издательства "БХВ-Петербург" в продаже:

Магазин "Новая техническая книга": СПб., Измайловский пр., д. 29, тел. (812) 251-41-10
Отдел оптовых поставок: e-mail: opt@bhv.spb.su

Серия «Профессиональное программирование»

Буторин Д. MS Agent и Speech API в Delphi (+CD-ROM)	448 с.
Гайдуков С. OpenGL. Профессиональное программирование трехмерной графики на C++ (+CD-ROM)	736 с.
Горнаков С. DirectX 9. Уроки программирования на C++ (+CD-ROM)	400 с.
Климов А. MS Agent. Графические персонажи для интерфейсов (+CD-ROM)	352 с.
Корнилов Е. Программирование шахмат и других логических игр (+CD-ROM)	272 с.
Корняков В. Программирование документов и приложений MS Office в Delphi (+CD-ROM)	496 с.
Магда Ю. Использование ассемблера для оптимизации программ на C++ (+CD-ROM)	496 с.
Мержевич Е. Ускорение работы сайта	384 с.
Михайлов А. 1С:Предприятие 7.7/8.0: системное программирование	336 с.
Несвижский В. Программирование аппаратных средств в Windows (+CD-ROM)	880 с.
Петюшкин А. HTML в Web-дизайне	400 с.
Пирогов В. MS SQL Server 2000: управление и программирование	608 с.
Плаугер П. STL – стандартная библиотека шаблонов C++	656 с.
Поляков А., Брусенцев В. Программирование графики: GDI+ и DirectX (+CD-ROM)	368 с.
Шилдт Г. Искусство программирования на C++	496 с.

Серия «Аппаратные средства»

Агуров П. Интерфейс USB. Практика использования и программирования (+CD-ROM)	576 с.

Серия «Системный администратор»

Бигелоу С. Сети: поиск неисправностей, поддержка и восстановление	1200 с.
Стахнов А. Сетевое администрирование Linux (+CD-ROM)	480 с.